Microsoft®
Advanced Group Policy Management

Microsoft Advanced Group Policy Management 4.0 操作指南

Microsoft Corporation

发布日期：2009 年 9 月

摘要

本指南提供使用 Microsoft 高级组策略管理 (AGPM) 4.0 执行任务的逐步说明。本指南包括 AGPM 帮助中的所有信息。

Microsoft

版权

目录

Microsoft Advanced Group Policy Management 4.0 操作指南

您可以使用 Microsoft 高级组策略管理 (AGPM) 扩展 组策略管理控制台 (GPMC) 的功能。AGPM 为 组策略对象 (GPO) 提供了全面的更改控制和改进的管理方法。

使用 AGPM 可以执行以下任务：

- 对 GPO 进行脱机编辑，以便可以创建 GPO 并在将其部署到生产环境之前对其进行测试。
- 在中央存档中维护 GPO 的多个版本，以便出现问题时可以回滚。
- 使用基于角色的委派在多人之间共享编辑、批准和审阅 GPO 的职责。
- 消除了多个组策略管理员使用 GPO 的签入和签出功能覆盖彼此所做工作的危险。
- 使用差异报告分析对 GPO 所做的更改，将该 GPO 与其他 GPO 或同一 GPO 的其他版本进行比较。
- 使用 GPO 模板简化创建新 GPO 的过程，存储通用策略设置和首选项设置以用作新 GPO 的起点。
- 委派对生产环境的访问权限。
- 搜索具有特定属性的 GPO，并筛选所显示的 GPO 列表。
- 将 GPO 导出到文件，以便可将其从测试林中的域复制到生产林中的域。

AGPM 在 GPMC 中显示的每个域下添加**“更改控制”**文件夹，还为在 GPMC 中显示的每个 GPO 和组策略链接添加**“历史记录”**选项卡。

- Advanced Group Policy Management 概述
- 版本控制的最佳做法
- 清单：管理 AGPM 服务器和存档
- 清单：创建、编辑和部署 GPO
- 搜索和筛选 GPO 列表
- 执行 AGPM 管理员任务
- 执行编辑任务
- 执行审批者任务
- 执行审阅者任务
- AGPM 疑难解答
- 用户界面：Advanced Group Policy Management

Advanced Group Policy Management 概述

您可以使用 高级组策略管理 (AGPM) 扩展 组策略管理控制台 (GPMC) 的功能，从而为 组策略对象 (GPO) 提供全面的更改控制和改进的管理方法。

组策略对象开发与更改控制

使用 AGPM，可以将每个 GPO 的副本存储在中央存档中，以便组策略管理员可以脱机查看和更改 GPO，而不会立即影响 GPO 的已部署版本。此外，AGPM 还会将每个受控 GPO 的每个版本的副本存储在存档中，以便您可以在需要时回滚到早期版本。

术语“签入”和“签出”与在库（或提供更改控制、版本控制或源控制进行编程开发的应用程序）中的使用方式相同。要使用库中的书籍，请在库中将其签出。签出后，其他人无法再使用该书籍。使用完成后，应将该书籍签入库中，这样其他人才可以使用。

使用 AGPM 开发 GPO 时，请执行以下操作：

1. 新建受控 GPO 或控制早先的非受控 GPO。
2. 签出 GPO，以便只有您可以更改它。
3. 编辑 GPO。
4. 签入已编辑的 GPO，以便其他人可以更改它或者对其进行部署。
5. 检查更改。
6. 将 GPO 部署到生产环境中。

基于角色委派

AGPM 提供了全面且易于使用的基于角色委派来管理对存档中 GPO 的访问权限。域级别权限使 AGPM 管理员 能够提供对单个域的访问权限而不提供对其他域的访问权限。基于 GPO 委派使 AGPM 管理员 能够提供对特定 GPO 的访问权限而不提供域范围的访问权限。

在 AGPM 中，有一些专门定义的角色：AGPM 管理员（完全控制）、审批者、编辑和审阅者。AGPM 管理员 角色包含所有其他角色的权限。默认情况下，只有审批者有权将 GPO 部署到域的生产环境，从而保护该环境不会被经验不足的编辑误操作。此外默认情况下，所有角色都包含审阅者角色，因此能够查看报告中的 GPO 设置。但是，AGPM 使 AGPM 管理员 极具灵活性，可以通过自定义 GPO 访问权限来满足组织需求。

在多个组策略管理员环境中进行委派

在多人可以更改 GPO 的环境中，AGPM 管理员 会按组或个人委派编辑、审批者和审阅者的权限。有关编辑和审批者的典型 GPO 开发过程，请参阅清单：创建、编辑和部署 GPO。

其他参考

- **Microsoft Advanced Group Policy Management 4.0 操作指南**

版本控制的最佳做法

Microsoft 高级组策略管理 (AGPM) 提供了 组策略对象 (GPO) 版本控制，与 Microsoft Visual SourceSafe® 提供源代码版本控制的方式非常类似。开发人员可以使用 Visual SourceSafe 管理每个源文件的多个版本。组策略管理员可以使用 AGPM 对 GPO 执行相同操作。使用 AGPM 时，组策略管理员应知道应用于任何版本控制系统的最佳做法：

- **日期和时间：**AGPM 为 GPO 的每个版本打上日期和时间戳。若要确保历史记录准确无误，尤其是在多个计算机上编辑 GPO 时，请确保每个计算机的时钟都与一个权威时间源同步。
- **完成编辑后签入 GPO：**编辑通常会在签出 GPO 后忘记将它们签入回存档。然而，这样会阻止其他组策略管理员更改该 GPO。请始终在完成编辑后立即将 GPO 签入回 AGPM。
- **经常保存更改：**编辑 GPO 时，请经常保存更改。大多数编辑都是签出 GPO，进行很多更改，然后将 GPO 签入存档。应定期将 GPO 签入存档，然后再将其签出。签入的详情可以像更改每个设置后签入 GPO（不建议）或进行多组相关更改后签入 GPO 那样大。这样，可以更好地存档每个 GPO 的历史记录，以帮助排查问题。
- **经常部署 GPO：**不要让尚未部署的新 GPO 和已编辑的 GPO 在存档中大量累积。应尽快部署新的和已编辑的 GPO，以便最大限度降低其对生产环境的影响。同时部署多个新的和已编辑的 GPO 可能会危害生产环境。
- **签入 GPO 时记录更改目的：**任何审阅者都可以比较 GPO 的版本以查看两个版本之间的特定更改。记录这些特定更改不会添加任何值。应记录更改的意图和目的，而不是记录审阅者通过查看差异报告所了解的内容。版本注释应将值添加到比较报告中并可帮助审阅者理解编辑更改 GPO 的原因。
- **在测试环境中测试 GPO：**将 GPO 部署到生产环境而不进行测试会具有风险。应在测试林的域中测试 GPO，然后将 GPO 导出到文件，再将文件导入生产林中的域。此外，还可以将 GPO 链接到包含测试计算机和用户的组织单位。在测试环境中验证每个 GPO 的功能是否正常，然后将 GPO 部署到生产环境。

其他参考

- **Microsoft Advanced Group Policy Management 4.0 操作指南**

清单：管理 AGPM 服务器和存档

在 高级组策略管理 (AGPM) 中，AGPM 服务和存档都由 AGPM 管理员（完全控制） 管理。以下是 AGPM 管理员 的典型任务。

常见任务	参考
委派对存档中的 组策略对象 (GPO) 的访问权限 。	[委派对存档的域级别访问权限] [委派对存档中单个 GPO 的访问权限]
备份存档以启用灾难恢复。	[备份存档]

不常见任务	参考
从备份还原存档以从灾难恢复。	[从备份中还原存档]
将 AGPM 服务和/或存档移动到不同的服务器。	[移动 AGPM 服务器和存档]
更改存档路径、AGPM 服务帐户或 AGPM 服务侦	[修改 AGPM 服务]

不常见任务	参考
听的端口。	
对 AGPM 服务器的常见问题进行疑难解答。	AGPM 疑难解答 配置日志记录和跟踪

其他参考

- Microsoft Advanced Group Policy Management 4.0 操作指南

清单：创建、编辑和部署 GPO

在多人使用 高级组策略管理 (AGPM) 更改 组策略对象 (GPO) 的环境中，AGPM 管理员（完全控制） 会按组或个人委派编辑、审批者和审阅者的权限。下面是编辑和审批者的典型 GPO 开发过程。

任务	参考
编辑请求创建新的 GPO，或审批者创建新的 GPO。	请求创建新的受控 GPO 创建新的受控 GPO
如果编辑请求创建 GPO，由审批者批准这一请求。	批准或拒绝挂起的操作
编辑从存档签出 GPO 的副本，以便其他任何人都不能修改 GPO。编辑对 GPO 进行更改，然后将修改的 GPO 签入存档。	脱机编辑 GPO
如果在测试林中进行开发，编辑可将 GPO 导出到一个文件，再将该文件传送到生产林，然后导入该文件。此外，编辑还可以将 GPO 链接到包含测试计算机和用户的组织单位。	使用测试环境
编辑请求将 GPO 部署到域的生产环境。	请求部署 GPO
审阅者，如审批者或编辑，对 GPO 进行分析。	执行审阅者任务
审批者批准 GPO 并将其部署到域的生产环境或拒绝 GPO。	批准或拒绝挂起的操作

其他参考

Microsoft Advanced Group Policy Management 4.0 操作指南

搜索和筛选 GPO 列表

在 高级组策略管理 (AGPM) 中，可以搜索 组策略对象 (GPO) 及其属性列表，以筛选所显示的 GPO 列表。例如，可以搜索具有特定名称、状态或注释的 GPO。还可以搜索上次由特定组策略管理员更改或在特定日期更改的 GPO。

执行复杂搜索

可以使用 *GPO 属性 1: 搜索字符串 1 GPO 属性 2: 搜索字符串 2...所有列搜索字符串*格式执行复杂搜索。搜索不区分大小写。

- **GPO 属性：**AGPM 的 GPO 列表中除**“计算机版本”**或**“用户版本”**以外的任何列标题。GPO 属性包括 GPO 名称、状态、最近更改 GPO 的用户、最近更改 GPO 的日期和时间、注释、GPO 状态以及 GPO 所应用的 WMI 筛选器。
- **搜索字符串：**要在指定列中搜索的文本。如果字符串包含空格，必须用引号将字符串引起来。
- **所有列搜索字符串：**要在 AGPM 的 GPO 列表中除**“计算机版本”**和**“用户版本”**以外的所有列中搜索的文本。可以包含多个以空格分隔的字符串。如果字符串包含空格，必须用引号将字符串引起来。

使用逻辑 AND 操作可以将每个 GPO 属性和搜索字符串对以及每个所有列搜索字符串组合在一起。搜索结果为符合以下条件的所有 GPO 的列表：每个指定的属性均包含指定的搜索字符串，并且至少有一列显示任何所有列搜索字符串。搜索将返回字符串的任何部分匹配项，以便您只需输入部分 GPO 名称或用户名，即可查看其名称中包括该文本的所有 GPO 的列表。

以下是搜索示例：

搜索结果描述	**搜索查询**
名称包括文本**安全**和**北美**的所有 GPO。	**名称: 安全 名称: ″北美″**
所有签出的 GPO。	**状态: ″已签出″**
由名为**管理员**的用户最近在上月更改的所有 GPO。	**更改者: 管理员 更改日期:** lastmonth
最近注释中包括词语**防火墙**且任何列中显示有词语**安全**的所有 GPO。	**注释: 防火墙 安全**
状态为**“已禁用所有设置”**的所有 GPO。	**GPO 状态: 全部**
应用了名为**我的 WMI 筛选器**的 WMI 筛选器且状态为**“已禁用用户配置设置”**的所有 GPO。	**WMI 筛选器: ″我的 WMI 筛选器″ GPO 状态: 用户**

指定日期

可以使用在 Windows 中搜索时可用的相同特殊术语搜索在特定日期、特定时间或时间范围内更改的 GPO。如果输入特定日期或时间，必须使用**“更改日期”**列中使用的格式。以下是搜索**“更改日期”**列的示例：

- **更改日期:10/10/2009**
- **更改日期:10/10/2009 9:00:00 AM**
- **更改日期:**thisweek

搜索**“更改日期”**列时，可以使用以下特殊术语（不区分大小写）：

- Today
- Yesterday
- ThisWeek
- LastWeek
- ThisMonth
- LastMonth
- TwoMonths
- ThreeMonths
- ThisYear
- LastYear

其他注意事项

- 默认情况下，只有审阅者、编辑、审批者或者 AGPM 管理员（完全控制），才能执行此过程。具体而言，您必须拥有域的**“列出内容”**权限。
- 有关 GPO 属性的详细信息，请参阅内容选项卡功能。

其他参考

- **Microsoft Advanced Group Policy Management 4.0 操作指南**

执行 AGPM 管理员任务

高级组策略管理 (AGPM) 允许 AGPM 管理员（完全控制） 配置域范围选项并委派审批者、编辑、审阅者和 AGPM 管理员 的权限。默认情况下，AGPM 管理员 是拥有完全控制权限（所有 AGPM 权限）的用户，因此也可以执行与任何角色相关的任务。

在多人开发 组策略对象 (GPO) 的环境中，您可以选择让所有组策略管理员执行相同的任务并具有相同的访问级别。或者，您可以选择让 AGPM 管理员 为可以更改 GPO 的编辑以及将 GPO 部署到生产环境的审批者委派权限。AGPM 管理员 可以配置权限以满足组织的需求。

- 配置 Advanced Group Policy Management：配置 AGPM 服务器连接和电子邮件通知，委派对生产环境中的 GPO 的访问权限，以及配置日志记录和跟踪以进行疑难解答。
- 管理存档：委派对存档中的 GPO 的访问权限，限制存储的每个 GPO 的版本数量，从其他域导入 GPO，以及备份和还原存档。

- 管理 AGPM 服务：停止并启动 AGPM 服务，或者更改存档路径、AGPM 服务帐户或 AGPM 服务侦听的端口。
- 移动 AGPM 服务器和存档：将 AGPM 服务和/或存档移动到不同的服务器。

注意
由于 AGPM 管理员 角色包含所有其他角色的权限，因此 AGPM 管理员 可以执行通常与任何其他角色相关的任务。

执行审批者任务，如创建、部署或删除 GPO

执行编辑任务，如编辑、重命名、导入 GPO 或为 GPO 加标签，创建模板，或者设置默认模板

执行审阅者任务，如检查设置和比较 GPO

其他注意事项

默认情况下，AGPM 管理员 角色拥有完全控制权限 - 所有 AGPM 权限：

- 列出内容
- 读取设置
- 编辑设置
- 创建 GPO
- 部署 GPO
- 删除 GPO
- 导出 GPO
- 导入 GPO
- 创建模板
- 修改选项
- 修改安全性

“修改选项”和**“修改安全性”**权限是 AGPM 管理员 角色独有的权限。

配置 Advanced Group Policy Management

在 高级组策略管理 (AGPM) 中，作为 AGPM 管理员（完全控制），您可以为组策略管理员集中配置 AGPM 服务器连接，配置 AGPM 的电子邮件通知、配置 AGPM 的可选电子邮件安全性，在域的生产环境中委派对 组策略对象 (GPO) 的访问权限，以及配置日志记录和跟踪进行疑难解答。

- 配置 AGPM 服务器连接
- 配置电子邮件通知
- 配置 AGPM 电子邮件安全性
- 委派对生产环境的访问权限
- 配置日志记录和跟踪

其他参考

- 有关委派对存档中 GPO 的访问权限的信息，请参阅管理存档。

- 有关如何限制存档中存储的每个 GPO 的版本数量的信息，请参阅限制存储的 GPO 版本。
- 执行 AGPM 管理员任务

配置 AGPM 服务器连接

每个受控 组策略对象 (GPO) 的所有版本都存储在中央存档中，以便组策略管理员可以脱机查看并修改 GPO，而不会直接对每个 GPO 的部署版本产生影响。

需要使用具有 AGPM 管理员（完全控制） 角色的用户帐户、创建在这些过程中使用的 GPO 的审批者的用户帐户或者具有 高级组策略管理 (AGPM) 中所需权限的用户帐户，才能完成这些为所有组策略管理员集中配置存档位置的过程。请在此主题的“其他考虑事项”中查看详细信息。

配置 AGPM 服务器连接

作为 AGPM 管理员，您可以通过集中配置关联设置，以确保所有组策略管理员都能连接到同一 AGPM 服务器。如果您的环境中某些域或所有域需要单独的 AGPM 服务器，除默认服务器以外还需配置这些其他的 AGPM 服务器。如果您没有集中配置 AGPM 服务器连接，那么每个组策略管理员必须手动配置每个域要显示的 AGPM 服务器。

- 为所有组策略管理员配置 AGPM 服务器连接
- 为所有组策略管理员配置其他 AGPM 服务器连接
- 为您的帐户手动配置 AGPM 服务器连接

对所有组策略管理员配置 AGPM 服务器连接

1. 在**“组策略管理控制台”**树中，编辑要应用于所有组策略管理员的 GPO。（有关详细信息，请参阅编辑 GPO。）
2. 在**“组策略管理编辑器”**窗口中，单击**“用户配置”**、**“策略”**、**“管理模板”**、**“Windows 组件”**和**“AGPM”**。
3. 在详细信息窗格中，双击**“AGPM:指定默认 AGPM 服务器(所有域)”**。
4. 在**“属性”**窗口中，选择**“已启用”**复选框，然后键入完全限定的计算机名称和端口（例如，server.contoso.com:4600）。
5. 单击**“确定”**。除非您要配置其他 AGPM 服务器连接，否则关闭**“组策略管理编辑器”**窗口，然后部署 GPO。（有关详细信息，请参阅部署 GPO。）当更新组策略时，会为所有组策略管理员配置 AGPM 服务器连接。

为所有组策略管理员配置其他 AGPM 服务器连接

1. 如果尚未配置任何 AGPM 服务器连接，则按照上述过程为配置所有域的默认 AGPM 服务器。
2. 要为某些域或所有域配置单独的 AGPM 服务器（覆盖默认 AGPM 服务器），请在**“组策略管理控制台”**树中编辑要适用于所有组策略管理员的 GPO。（有关详细信息，请参阅编辑 GPO。）
3. 在**“组策略管理编辑器”**窗口中，单击**“用户配置”**、**“策略”**、**“管理模板”**、**“Windows 组件”**和**“AGPM”**。

4. 在详细信息窗格中，双击**“AGPM:指定 AGPM 服务器”**。
5. 在**“属性”**窗口中，选中**“已启用”**复选框，然后单击**“显示”**。
6. 在**“显示内容”**窗口中：
   a. 单击**“添加”**。
   b. 在**“值名称”**中，键入域名（例如，server1.contoso.com）。
   c. 在**“值”**中，键入用于此域的 AGPM 服务器名称和端口（例如，server2.contoso.com:4600），然后单击**“确定”**。（默认情况下，AGPM 服务侦听端口 4600。若要使用其他端口，请参阅修改 AGPM 服务。）
   d. 为不使用默认 AGPM 服务器的每个域重复以上步骤。
7. 单击**“确定”**，关闭**“显示内容”**和**“属性”**窗口。
8. 关闭**“组策略管理编辑器”**窗口。（有关详细信息，请参阅部署 GPO。）当更新组策略时，会为所有组策略管理员配置新的 AGPM 服务器连接。

如果已集中配置 AGPM 服务器连接，则所有组策略管理员的手动配置选项将不可用。

为您的帐户手动配置要显示的 AGPM 服务器

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中，单击**“AGPM 服务器”**选项卡。
3. 为管理用于此域的存档的 AGPM 服务器输入完全限定的计算机名称（例如，server.contoso.com）和 AGPM 服务监听的端口（默认为端口 4600）。
4. 单击**“应用”**，然后单击**“是”**进行确认。

其他注意事项

- 您必须能够编辑并部署 GPO，才能执行为所有组策略管理员集中配置 AGPM 服务器连接的过程。有关其他详细信息，请参阅编辑 GPO 和部署 GPO。
- 所选 AGPM 服务器确定在**“内容”**选项卡上显示的 GPO，以及**“域委托”**选项卡设置应用的位置。如果不通过管理模板进行集中管理，则每个组策略管理员必须配置此设置，才能指向域的 AGPM 服务器。
- Group Policy Creator Owners 组中的成员身份应加以限制，确保不会危害能够访问 GPO 的 AGPM 管理。（在“组策略管理控制台”中，单击您要在其中管理 GPO 的林和域的“组策略对象”，单击“委派”，然后配置设置以满足您的组织的需求。）

其他参考

- 配置 Advanced Group Policy Management

配置电子邮件通知

当编辑或审阅者尝试创建、部署或者删除 组策略对象 (GPO) 时，关于此操作的请求会发送到指定的电子邮件地址，这样审批者可以评估请求，然后执行或拒绝请求。您应确定要接收通知的电子邮件地址，以及用来发送通知的别名。

若要完成此过程，必须使用 AGPM 管理员（完全控制） 角色的或拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的"其他考虑事项"中查看详细信息。

配置 AGPM 的电子邮件通知

1. 在"**组策略管理控制台**"树中，单击您要在其中管理 GPO 的林和域中的"**更改控制**"。
2. 在详细信息窗格中，单击**"域委托"**选项卡。
3. 在**"发件人电子邮件地址"**字段中，键入将用来发送通知的 AGPM 电子邮件别名。
4. 在**"收件人电子邮件地址"**字段中，键入应接收要批准的请求的审批者的电子邮件地址逗号分隔列表。
5. 在**"SMTP 服务器"**字段中，键入有效的 SMTP 邮件服务器。
6. 在**"用户名"**和**"密码"**字段中，键入拥有 SMTP 服务访问权限的用户凭证。
7. 单击**"应用"**。

其他注意事项

- 默认情况下，您必须是 AGPM 管理员（完全控制） 才能执行此过程。具体而言，您必须拥有域的**"列出内容"**和**"修改选项"**权限。
- AGPM 电子邮件通知是域级别设置。您可以在每个域的**"域委托"**选项卡上提供不同审批者的电子邮件地址或 AGPM 电子邮件别名，也可以在您的整个环境中使用相同的电子邮件地址。
- 默认情况下，电子邮件在发送时是作为 高级组策略管理 (AGPM) 中的操作结果而未进行加密的。但是，您可以使用注册表设置配置 AGPM 电子邮件安全性，指定是否使用安全套接字层 (SSL) 加密和要使用的 SMTP 端口。有关详细信息，请参阅配置 AGPM 电子邮件安全性。

其他参考

- 配置 Advanced Group Policy Management

配置 AGPM 电子邮件安全性

默认情况下，由于 高级组策略管理 (AGPM) 中的操作而发送的电子邮件通知没有经过加密，而且是通过 SMTP 端口 25 发送的。但是，您可以使用注册表设置配置 AGPM 电子邮件的安全性，指定是否使用安全套接字层 (SSL) 加密以及要使用的 SMTP 端口。

通过对 AGPM 电子邮件通知进行加密，可以更好地保护可能会显示有关组织安全性的敏感信息的电子邮件。如果要通过远程邮件服务器中继电子邮件，建议对电子邮件通知进行加密，并且某些合规性可能要求对电子邮件通知进行加密。

注意

不正确地编辑注册表可能会对系统造成严重损坏。更改注册表之前，应对计算机上的所有重要数据进行备份。

要完成这些过程，需要使用具有 AGPM 管理员（完全控制） 角色的用户帐户（即创建在这些过程中使用的 组策略对象 (GPO) 的审批者的用户帐户），或者拥有 AGPM 中所需权限的用户帐户。请在此主题的"其他考虑事项"中查看详细信息。

使用组策略首选项配置 AGPM 电子邮件安全性

1. 在**“组策略管理控制台”**树中，编辑应用于要配置电子邮件安全性的所有 AGPM 服务器的 GPO。（有关详细信息，请参阅编辑 GPO。）
2. 在**“组策略管理编辑器”**窗口中，展开**“计算机配置”**、**“首选项”**、**“Windows 设置”**和**“注册表”**文件夹。
3. 在控制台树中，右键单击**“注册表”**，指向**“新建”**，单击**“集合项目”**，然后键入**“AGPM 电子邮件安全性”**。
4. 创建启用加密的注册表首选项项目：
    a. 在控制台树中，右键单击**“AGPM 电子邮件安全性”**，指向**“新建”**，然后单击**“注册表项”**。
    b. 在**“新注册表属性”**对话框中，选择**“更新”**操作。
    c. 对于**“配置单元”**，选择**“HKEY_LOCAL_MACHINE”**。
    d. 对于**“注册表项路径”**，键入**“SOFTWARE\Microsoft\AGPM”**。
    e. 对于**“值名称”**，键入**“EncryptSmtp”**。
    f. 对于**“值类型”**，选择**“REG_DWORD”**。
    g. 对于**“基数”**，选择**“小数”**，对于**“数值数据”**，键入**“1”**以使用 SSL 加密，或者键入**“0”**允许不加密就发送电子邮件。默认情况下，不加密就发送电子邮件。单击**“确定”**。
5. 创建指定 SMTP 端口的注册表首选项项目：
    a. 在控制台树中，右键单击**“AGPM 电子邮件安全性”**，指向**“新建”**，然后单击**“注册表项”**。
    b. 在**“新注册表属性”**对话框中，选择**“更新”**操作。
    c. 对于**“配置单元”**，选择**“HKEY_LOCAL_MACHINE”**。
    d. 对于**“注册表项路径”**对话框，键入**“SOFTWARE\Microsoft\AGPM”**。
    e. 对于**“值名称”**，键入**“SmtpPort”**。
    f. 对于**“值类型”**，选择**“REG_DWORD”**。
    g. 对于**“基数”**，选择**“小数”**，对于**“数值数据”**，键入 SMTP 端口的端口号。默认情况下，未启用加密时 SMTP 端口是 25，启用加密时是 587。单击**“确定”**。
6. 关闭**“组策略管理编辑器”**窗口，然后签入并部署 GPO。有关详细信息，请参阅部署 GPO。

其他注意事项

- 必须能使用组策略首选项编辑和部署 GPO 以配置注册表设置。有关其他详细信息，请参阅编辑 GPO 和部署 GPO。

其他参考

- 配置 Advanced Group Policy Management

委派对生产环境的访问权限

在 高级组策略管理 (AGPM) 中，可以更改域的生产环境中的 组策略对象 (GPO) 的访问权限，替换那些 GPO 上的任何现有权限。可以在域级别将权限配置为，当用户不使用 组策略管理控制台

(GPMC) 中的**“更改控制”**文件夹时，允许或阻止用户编辑、删除或修改生产环境中的 GPO 的安全性。

注意

- 更改生产环境的访问权限的委派方式不会影响用户链接 GPO 的能力。
- 当 GPO 为受控或已部署时，就会删除其他所有帐户的访问权限，但拥有**“读取”**和**“应用”**权限的除外。

若要完成此过程，需要使用拥有 AGPM 管理员（完全控制） 角色或拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

在域的生产环境中更改对 GPO 的访问权限

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 单击**“生产委托”**选项卡。
3. 要为没有生产环境访问权限的用户或组添加权限，或者替换拥有生产环境访问权限的用户或组的权限，请按以下步骤操作：
   a. 单击**“添加”**，选择用户或组，然后单击**“确定”**。
   b. 选择要在生产环境中为该用户或组委派的权限，然后单击**“确定”**。
4. 若要删除用户或组在生产环境中的所有权限，请选择用户或组，单击**“删除”**，然后单击**“确定”**。

其他注意事项

- 默认情况下，您必须是 AGPM 管理员（完全控制） 才能执行此过程。明确地说，您必须拥有域的**“修改安全性”**权限。
- 不能在**“生产委托”**选项卡上更改 AGPM 服务帐户的权限。
- 默认情况下，下列帐户拥有生产环境中 GPO 的权限：

帐户	**GPO 的默认权限**
<AGPM 服务帐户>	编辑设置、删除和修改安全性
经过身份验证的用户	读取、应用
域管理员	编辑设置、删除和修改安全性
企业管理员	编辑设置、删除和修改安全性
企业域控制器	读取
系统	编辑设置、删除和修改安全性

- Group Policy Creator Owners 组中的成员身份应加以限制，确保不会危害能够访问 GPO 的 AGPM 管理。（在“组策略管理控制台”中，单击您要在其中管理 GPO 的林和域的“组策略对象”，单击“委派”，然后配置设置以满足您的组织的需求。）

其他参考

- 配置 Advanced Group Policy Management

配置日志记录和跟踪

可以使用管理模板有选择地集中配置日志记录和跟踪。这对于诊断与 高级组策略管理 (AGPM) 相关的任何问题可能很有帮助。

要完成这些过程，需要使用具有 AGPM 管理员（完全控制） 角色的用户帐户（即创建在这些过程中使用的 组策略对象 (GPO) 的审批者的用户帐户），或者拥有 AGPM 中所需权限的用户帐户。此外，需要使用具有 AGPM 服务器访问权限的用户帐户，才能初始化 AGPM 服务器上的日志记录。请在此主题的"其他考虑事项"中查看详细信息。

配置 AGPM 的日志记录和跟踪

1. 在**"组策略管理控制台"**树中，编辑将应用于需要启用日志记录和跟踪的所有组策略管理员的 GPO。（有关详细信息，请参阅编辑 GPO。）
2. 在**"组策略管理编辑器"**窗口中，单击**"计算机配置"**、**"策略"**、**"管理模板"**、**"Windows 组件"**和**"AGPM"**。
3. 在详细信息窗格中，双击**"AGPM:配置日志记录"**。
4. 在**"属性"**窗口中，单击**"已启用"**，然后配置将在日志中记录的详细信息的级别。
5. 单击**"确定"**。
6. 关闭**"组策略管理编辑器"**窗口。（有关详细信息，请参阅部署 GPO。）在更新组策略后，只有重新启动 AGPM 服务，才能启动、修改或停止 AGPM 服务器上的日志记录。组策略管理员只有关闭并重新启动 GPMC，才能启动、修改或者停止其计算机上的日志记录。

   跟踪文件位置：

   - 客户端：%LocalAppData%\Microsoft\AGPM\agpm.log
   - 服务器：%ProgramData%\Microsoft\AGPM\agpmserv.log

其他注意事项

- 必须能够编辑和部署 GPO，才能配置 AGPM 日志记录和跟踪。有关其他详细信息，请参阅编辑 GPO 和部署 GPO。

其他参考

- 配置 Advanced Group Policy Management

管理存档

在 高级组策略管理 (AGPM) 中，作为 AGPM 管理员（完全控制），您需管理存档的访问权限，并可以限制存档中存储的每个 组策略对象 (GPO) 的版本数量。您可以在域级别或 GPO 级别委派对存档中 GPO 的访问权限。此外，还可以备份存档，以便在发生灾难时或许能够恢复存档。

作为 AGPM 管理员，可以将 GPO 导出到一个文件，再将该文件复制到其他林，然后将该 GPO 导入该林中的某个域。与编辑不同，在创建新受控 GPO 时，您可以将策略设置直接从 GPO 备份导入该新受控 GPO。有关如何导出 GPO 的信息，请参阅将 GPO 导出到文件。

- 委派对存档的域级别访问权限

- 委派对存档中单个 GPO 的访问权限
- 限制存储的 GPO 版本
- 从文件中导入 GPO
- 备份存档
- 从备份中还原存档

其他参考

- 有关如何对生产环境中的 GPO 委派访问权限的信息，请参阅委派对生产环境的访问权限。
- 有关如何移动存档的信息，请参阅移动 AGPM 服务器和存档。
- 执行 AGPM 管理员任务

委派对存档的域级别访问权限

设置对您的环境的委派，以便组策略管理员对存档中的 组策略对象 (GPO) 具有适当的访问和控制权限。您可以应用一些基本权限来使操作更有效。可以采用任何满足组织的需要的方式来授予权限。

若要完成此过程，必须使用 AGPM 管理员（完全控制） 角色的或拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

通过委派访问权限使用户和组对整个域中的所有 GPO 拥有适当的权限

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 单击“**域委托**”选项卡，配置对域中所有 GPO 的访问权限：
   a. 若要为用户或组添加访问权限，请单击“**添加**”按钮，选择相应用户或组，然后单击“**确定**”。在“**添加组或用户**”对话框中，选择角色并单击“**确定**”。
   b. 若要删除用户或组的访问权限，请选择相应用户或组，然后单击“**删除**”按钮。
   c. 要修改委派给用户或组的角色和权限，请选择单击“**高级**”按钮。在“**权限**”对话框中，选择用户或组，选中要分配给该用户或组的每个角色对应的复选框，然后单击“**确定**”。

   备注

   编辑和审批者的权限包括审阅者的权限。

其他注意事项

- 默认情况下，您必须是 AGPM 管理员（完全控制） 才能执行此过程。明确地说，您必须拥有域的“**修改安全性**”权限。
- 若要将读取访问权限委托给使用 AGPM 的组策略管理员，则必须授予他们“**列出内容**”及“**读取设置**”权限。他们使用该权限可以查看 AGPM 的“**内容**”选项卡上的 GPO。其他权限必须明确委托。
- 编辑必须被授予 GPO 的已部署副本的“**读取**”权限，才能完整地使用组策略软件安装。

- Group Policy Creator Owners 组中的成员身份应加以限制，确保不会危害能够访问 GPO 的 AGPM 管理。（在“组策略管理控制台”中，单击您要在其中管理 GPO 的林和域的“组策略对象”，单击“委派”，然后配置设置以满足您的组织的需求。）

其他参考

- 管理存档

委派对存档中单个 GPO 的访问权限

作为 AGPM 管理员（完全控制），您可以委派管理存档中的受控 组策略对象 (GPO)，以便选定的组和编辑可以进行编辑，审阅者可以进行审阅，审批者可以加以批准。

若要完成此过程，必须使用具有 AGPM 管理员（完全控制） 角色的用户帐户、创建 GPO 的审批者的用户帐户，或者具有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

委托受控 GPO 的管理

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格的**“内容”**选项卡上，单击**“受控”**选项卡以显示受控 GPO，然后单击 GPO 进行委托：
   a. 若要为用户或组添加访问权限，请单击**“添加”**按钮，选择相应用户或组，然后单击**“确定”**。在**“添加组或用户”**对话框中，选择角色并单击**“确定”**。
   b. 若要删除用户或组的访问权限，请选择相应用户或组，然后单击**“删除”**按钮。

      备注

      如果用户或组继承域范围内的访问权限，则**“删除”**按钮不可用。可以在**“域委托”**选项卡上修改域范围内的访问权限。

   c. 若要修改委托给用户或组的角色和权限，请单击**“高级”**按钮。在**“权限”**对话框中，选择相应用户或组，选中每个要分配给该用户或组的角色旁的复选框，然后单击**“确定”**。

      备注

      编辑和审批者的权限包括审阅者的权限。

其他注意事项

- 默认情况下，您必须是创建或控制 GPO 的审批者或 AGPM 管理员（完全控制） 才能执行此过程。具体而言，您必须拥有域的**“列出内容”**权限和 GPO 的**“修改安全性”**权限。
- 若要将读取访问权限委托给使用 AGPM 的组策略管理员，则必须授予他们**“列出内容”**及**“读取设置”**权限。他们使用该权限可以查看 AGPM 的**“内容”**选项卡上的 GPO。其他权限必须明确委托。
- 编辑必须拥有已部署 GPO 副本的**“读取”**权限，才能充分利用组策略软件安装。
- Group Policy Creator Owners 组中的成员身份应加以限制，确保不会危害能够访问 GPO 的 AGPM 管理。（在“组策略管理控制台”中，单击您要在其中管理 GPO 的林和域的“组策略对象”，单击“委派”，然后配置设置以满足您的组织的需求。）

其他参考

- 管理存档

限制存储的 GPO 版本

默认情况下，每个受控 组策略对象 (GPO) 的所有版本都会保留在 AGPM 服务器上的存档中。但是，您可以限制为每个 GPO 保留的版本数量，并在超出限制时删除较旧版本。当删除 GPO 版本后，该版本的记录会保留在 GPO 的历史记录中，但 GPO 版本本身会从存档中删除。

若要完成此过程，必须使用 AGPM 管理员（完全控制） 角色的或拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

限制 GPO 版本的存储数量

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中，单击“**AGPM 服务器**”选项卡。
3. 选中“**从存档中删除每个 GPO 的旧版本**”复选框，并键入要为每个 GPO 存储的最大 GPO 版本数量，其中不包括当前版本。若要仅保留当前版本，请输入 0。最大数不能大于 999。

   重要事项

   此限制仅计算“**历史记录**”窗口的“**唯一版本**”选项卡上显示的 GPO 版本。
4. 单击“**应用**”按钮。

其他注意事项

- 默认情况下，您必须是 AGPM 管理员（完全控制） 才能执行此过程。具体而言，您必须拥有域的“**列出内容**”和“**修改选项**”权限。
- 您可以在历史记录中将某个 GPO 版本标记为不可删除来防止该 GPO 版本被删除。为此，请在 GPO 历史记录中右键单击该版本并单击“**不删除**”。

其他参考

- 管理存档

从文件中导入 GPO

在 高级组策略管理 (AGPM) 中，如果您是 AGPM 管理员（完全控制） 并且已将 组策略对象 (GPO) 导出到 CAB 文件，则可以将该 GPO 的策略设置导入其他林的域中的新 GPO 或现有 GPO。有关将 GPO 设置导出到 CAB 文件的信息，请参阅将 GPO 导出到文件。

若要将策略设置导入新的受控 GPO，则需要使用具有 AGPM 管理员 角色或具有 AGPM 中必需权限的用户帐户。若要将策略设置导入现有 GPO，则需要使用具有编辑或 AGPM 管理员 角色，或者具有 AGPM 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

从文件导入策略设置

从文件导入策略设置时，可以将策略设置导入新 GPO 或现有 GPO。但是，如果将策略设置导入现有 GPO，将替换该 GPO 中的所有策略设置。

- 将策略设置导入新的受控 GPO

- 将策略设置导入现有 GPO

将策略设置导入新的受控 GPO

1. 在**“组策略管理控制台”**树中，单击要将策略设置导入的域中的**“更改控制”**。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 创建新的受控 GPO。在**“新建受控 GPO”**对话框中，单击**“导入”**，然后单击**“启动向导”**。有关如何创建 GPO 的详细信息，请参阅创建新的受控 GPO。
4. 按照**“导入设置向导”**中的说明选择 GPO 备份，从其中为新 GPO 导入策略设置，然后输入新 GPO 的审计跟踪的注释。

将策略设置导入现有 GPO

1. 在**“组策略管理控制台”**树中，单击要将策略设置导入的域中的**“更改控制”**。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 签出要将策略设置导入的目标 GPO。
4. 右键单击目标 GPO，指向**“导入自”**，然后单击**“文件”**。
5. 按照**“导入设置向导”**中的说明选择 GPO 备份，导入其策略设置以替换目标 GPO 中的策略设置，然后输入目标 GPO 的审计跟踪的注释。默认情况下，向导完成后将签入目标 GPO。

其他注意事项

- 若要将策略设置导入新的受控 GPO，您必须拥有域的**“列出内容”**、**“导入 GPO”**和**“创建 GPO”**权限。默认情况下，您必须是 AGPM 管理员 才能执行此过程。
- 若要将策略设置导入现有 GPO，您必须拥有域的**“列出内容”**、**“编辑设置”**和**“导入 GPO”**权限，且该 GPO 必须由您签出。默认情况下，必须是编辑者或 AGPM 管理员（完全控制）才能执行此过程。

其他参考

- 管理存档

备份存档

若要在出现灾难时帮助恢复 高级组策略管理 (AGPM) 的存档，AGPM 管理员（完全控制） 应经常备份存档。默认情况下，会在 %ProgramData%\Microsoft\AGPM 中创建存档。但是，您可以在安装 Microsoft Advanced Group Policy Management - Server 时指定其他路径。

要完成此过程，需要使用同时对 AGPM 服务器（安装 AGPM 服务的计算机）和包含存档的文件夹具有访问权限的用户帐户。

备份存档

1. 停止 AGPM 服务。有关详细信息，请参阅启动和停止 AGPM 服务。
2. 使用 Windows 资源管理器、Xcopy、Windows Server® Backup 或其他备份工具备份存档文件夹。确保备份隐藏文件、系统文件和只读文件。

3. 将存档备份存储到安全位置。
4. 重新启动 AGPM 服务。有关详细信息，请参阅启动和停止 AGPM 服务。

备注

如果 AGPM 管理员 未经常备份存档，存档备份中的 组策略对象 (GPO) 将不是最新的。若要更好地确保存档备份是最新的，请将备份存档作为组织日常备份策略的一部分。

其他参考

- 从备份中还原存档
- 移动 AGPM 服务器和存档
- 管理存档

从备份中还原存档

如果发生灾难且 高级组策略管理 (AGPM) 的存档受损或遭到破坏，AGPM 管理员（完全控制） 可以从预先准备的备份副本还原存档，然后从域的生产环境导入不在存档中或其生产中的版本比存档中的版本更新的任何 组策略对象 (GPO)。有关如何将存档备份还原到其他服务器的信息，请参阅移动 AGPM 服务器和存档。

要完成此过程，需要使用同时对 AGPM 服务器（安装 AGPM 服务的计算机）和包含存档的文件夹具有访问权限的用户帐户。

从备份还原存档

1. 停止 AGPM 服务。有关详细信息，请参阅启动和停止 AGPM 服务。
2. 删除现有存档。默认情况下，存档文件夹为 %ProgramData%\Microsoft\AGPM，但是安装 Microsoft Advanced Group Policy Management - Server 的 AGPM 管理员 可能会在安装期间输入其他位置。
3. 通过配置存档路径、AGPM 服务帐户、存档所有者和侦听端口重新创建存档文件夹。不必使用原始安装期间使用的相同值。有关详细信息，请参阅修改 AGPM 服务。
4. 将存档备份的内容复制到存档文件夹，复制子文件夹和文件以确保每个子文件夹和文件都继承存档文件夹的权限。请小心不要覆盖存档文件夹。
5. 如果不确定存档备份中的 GPO 是否比生产中该 GPO 的副本新，请生成差异报告并比较其设置。有关详细信息，请参阅识别 GPO、GPO 版本或模板之间的差异。
6. 重新启动 AGPM 服务。有关详细信息，请参阅启动和停止 AGPM 服务。

其他参考

- 备份存档
- 移动 AGPM 服务器和存档
- 管理存档

管理 AGPM 服务

AGPM 服务是一项作为安全代理的 Windows 服务，用于管理客户端对存档和域的生产环境中的 组策略对象 (GPO) 的访问权限。它强制 高级组策略管理 (AGPM) 进行委派并提供增强级别的安全性。AGPM 服务位于安装 Microsoft Advanced Group Policy Management - Server 的服务器上。

注意

不要通过操作系统中的“管理工具”和“服务”修改 AGPM Service 的设置。这样做会阻止 AGPM Service 启动。

- 启动和停止 AGPM 服务
- 修改 AGPM 服务

其他参考

- 移动 AGPM 服务器和存档
- 执行 AGPM 管理员任务

启动和停止 AGPM 服务

AGPM 服务是一项作为安全代理的 Windows 服务，用于管理客户端对存档和生产环境中的 组策略对象 (GPO) 的访问。

重要事项

停止或禁用 AGPM 服务将防止 AGPM 客户端通过服务器执行任何操作（如列出 GPO 或编辑 GPO）。

若要完成此过程，必须使用拥有 AGPM 服务器（安装 AGPM 服务的计算机）的访问权限的用户帐户。

开始或停止 AGPM 服务

1. 在安装 Microsoft Advanced Group Policy Management - Server（因而安装了 AGPM 服务）的计算机上，依次单击**“开始”**、**“控制面板”**、**“管理工具”**，然后单击**“服务”**。
2. 在服务列表中，右键单击**“AGPM 服务”**，依次选择**“开始”**、**“重新启动”**或**“停止”**。

   注意

   不要通过操作系统中的“管理工具”和“服务”修改 AGPM Service 的设置。这样做会阻止 AGPM Service 启动。

其他参考

- 管理 AGPM 服务

修改 AGPM 服务

AGPM 服务是一项作为安全代理的 Windows 服务，用于管理客户端对存档和域的生产环境中的 组策略对象 (GPO) 的访问权限。如果此服务已停止或禁用，AGPM 客户端就不能通过服务器执行操作。您可以修改存档路径、AGPM 服务帐户和 AGPM 服务监听的端口。

注意

不要通过操作系统中的"管理工具"和"服务"修改 AGPM Service 的设置。这样做会阻止 AGPM Service 启动。

要完成此过程，所使用的用户帐户需为域管理组成员，并且具有 AGPM 服务器（安装了 Microsoft Advanced Group Policy Management - Server）的访问权限。另外，必须提供 AGPM 服务帐户的凭证，才能完成此过程。

修改 AGPM 服务

1. 在安装 Microsoft Advanced Group Policy Management - Server 的计算机上，单击**"开始"**、**"控制面板"**、**"程序"**以及**"程序和功能"**。
2. 右键单击**"Microsoft Advanced Group Policy Management - Server"**，然后单击**"更改"**。
3. 单击**"下一步"**，然后单击**"修改"**。
4. 按照说明配置 AGPM 服务：
   a. 在**"存档路径"**对话框中，输入 AGPM 服务器相关存档的新位置，或者确认当前存档路径，然后单击**"下一步"**。

      重要事项

      存档路径可以指向 AGPM 服务器上的一个文件夹或其他位置，但是该位置应该有充足的空间，才能存储此 AGPM 服务器管理的所有 GPO 和历史记录数据。

   b. 在**"AGPM 服务帐户"**对话框中，输入将运行 AGPM 服务的服务帐户的凭证，然后单击**"下一步"**。

      重要事项

      修改安装时会清除 AGPM 服务帐户的凭证。必须重新输入凭证，但是不要求凭证与原始安装期间使用的凭证相匹配。

      AGPM 服务帐户必须具有访问将管理的 GPO 的全部权限，并且将被授予**"作为服务登录"**权限。如果要管理单一域上的 GPO，则可以将主节点域控制器的本地系统帐户用作 AGPM 服务帐户。

      如果要管理多个域上的 GPO，或者成员服务器为 AGPM 服务器，则应配置另一帐户作为 AGPM 服务帐户，因为一个域控制器的本地系统帐户不能访问其他域上的 GPO。

   c. 在**"存档所有者"**对话框中，输入 AGPM 管理员（完全控制） 或 AGPM 管理员 组的用户名，然后单击**"下一步"**。

      备注

      修改安装时会清除存档所有者的凭证。必须重新输入凭证，但是不要求凭证与原始安装期间使用的凭证相匹配。

   d. 在**"端口配置"**对话框中，键入 AGPM 服务应监听的新端口，或者确认当前选择的端口，然后单击**"下一步"**。

注意

默认情况下，AGPM 服务监听端口 4600。

如果您手动配置端口例外或拥有规则配置端口例外，则可以清除**“向防火墙添加端口例外”**复选框。

5. 单击**“更改”**，在安装完成后单击**“完成”**。
6. 如果更改了 AGPM 服务监听的端口，请修改每个组策略管理员的 AGPM 服务器连接中的端口。（有关详细信息，请参阅配置 AGPM 服务器连接。）
7. 为应当应用配置更改的各个 AGPM 服务器重复以上步骤。

其他参考

- 管理 AGPM 服务

移动 AGPM 服务器和存档

如果您要替换 AGPM 服务器和托管存档的服务器，必须移动 AGPM 服务和存档。如果您愿意，可以单独移动 AGPM 服务和存档。

注意

- AGPM 服务器是托管 AGPM 服务且安装了 Microsoft Advanced Group Policy Management – Server 的计算机。
- 默认情况下，将在 AGPM 服务器上托管存档，但您可以指定存档路径以在其他服务器上进行托管。

要完成此过程，所使用的用户帐户需为域管理组成员，并且具有以前和新 AGPM 服务器的访问权限。另外，必须提供要由新 AGPM 服务器使用的 AGPM 服务帐户的凭据，才能完成此过程。

将 AGPM 服务和存档移动到不同的服务器

1. 备份存档。有关详细信息，请参阅备份存档。
2. 移动 AGPM 服务：
   a. 停止 AGPM 服务。有关详细信息，请参阅启动和停止 AGPM 服务。
   b. 在将托管 AGPM 服务的新服务器上安装 Microsoft Advanced Group Policy Management - Server。在此过程中，需指定新的存档路径以及与 AGPM 服务器相关的存档的位置。有关详细信息，请参阅 Microsoft Advanced Group Policy Management 4.0 逐步指南 (http://go.microsoft.com/fwlink/?LinkId=153505) 和 Microsoft Advanced Group Policy Management 计划指南 (http://go.microsoft.com/fwlink/?LinkId=156883)。
   c. AGPM 管理员（完全控制） 必须为将使用新 AGPM 服务器的所有组策略管理员配置 AGPM 服务器连接，然后删除旧 AGPM 服务器的连接，或者组策略管理员必须手动配置新 AGPM 服务器连接，然后删除其计算机上的 AGPM 管理单元的旧 AGPM 服务器连接。有关详细信息，请参阅配置 AGPM 服务器连接。

      备注

作为最佳做法，应从以前的 AGPM 服务器上卸载 Microsoft Advanced Group Policy Management – Server。这将确保 AGPM 服务不会在该服务器上意外重新启动，并且在保留了该服务的任何 AGPM 服务器连接时不会导致混淆。

3. 将存档从备份复制到将托管该存档的新服务器。有关详细信息，请参阅从备份中还原存档。

重要事项

如果在移动存档时未移动 AGPM 服务：

a. 必须更改存档路径以指向与 AGPM 服务器相关的新存档位置。有关详细信息，请参阅修改 AGPM 服务。

b. 必须在**“域委托”**选项卡上重新输入密码并确认。有关详细信息，请参阅配置电子邮件通知。

其他参考

- 备份存档
- 从备份中还原存档
- 配置 AGPM 服务器连接
- 修改 AGPM 服务
- Microsoft Advanced Group Policy Management 4.0 逐步指南 (http://go.microsoft.com/fwlink/?LinkId=153505)
- Microsoft Advanced Group Policy Management 计划指南 (http://go.microsoft.com/fwlink/?LinkId=156883)
- 执行 AGPM 管理员任务

执行编辑任务

在 高级组策略管理 (AGPM) 中，编辑是经 AGPM 管理员（完全控制） 授权更改 组策略对象 (GPO) 和创建 GPO 模板的人员。此外，编辑还可以请求创建、删除或还原 GPO。审批者必须批准请求才能使请求得以执行。编辑可以将 GPO 导出到文件以便可将 GPO 复制到其他林中的域，并且可以导入从其他域复制的 GPO。

重要事项

确保您已连接到 GPO 的中央存档。有关详细信息，请参阅配置 AGPM 服务器连接。

- 创建或控制 GPO
- 编辑 GPO
- 使用测试环境
- 请求部署 GPO
- 创建模板和设置默认模板
- 删除或还原 GPO

备注

因为编辑角色包括审阅者角色的权限，所以编辑还可以查看设置和比较 GPO。有关详细信息，请参阅执行审阅者任务。

其他注意事项

默认情况下，为编辑角色提供下列权限：

- 列出内容
- 读取设置
- 编辑设置
- 导出 GPO
- 导入 GPO
- 创建模板

创建或控制 GPO

要使用 高级组策略管理 (AGPM) 提供 组策略对象 (GPO) 更改控制，必须先使 GPO 受控于 AGPM。在**“更改控制”**文件夹中创建的新 GPO 将自动成为受控 GPO。作为编辑，您可能没有完成控制、创建或删除 GPO 操作的权限，但是具有开始该过程并向审批者提交请求所需的权限。

- 请求控制非受控 GPO
- 请求创建新的受控 GPO
- 从生产中导入 GPO

请求控制非受控 GPO

要提供现有 组策略对象 (GPO) 的更改控制，该 GPO 必须是受控的。如果您不是审批者或 AGPM 管理员（完全控制），则必须请求对 GPO 进行控制。

若要完成此过程，必须使用编辑或审阅者角色的或者拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

控制非受控 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格的**“内容”**选项卡上，单击**“非受控”**选项卡以显示非受控 GPO。
3. 右键单击要使用 AGPM 控制的 GPO，然后单击**“控制”**。
4. 如果您没有控制 GPO 的特殊权限，则必须提交一个控制请求。若要接收请求的副本，请在**“抄送”**字段中键入您的电子邮件地址。键入将在 GPO 的**“历史记录”**中显示的注释，然后单击**“提交”**。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。GPO 已从**“非受控”**选项卡上的列表中删除且添加到**“挂起”**选项卡上。当审批者批准您的请求后，GPO 将被移到**“受控”**选项卡。

其他注意事项

- 默认情况下，您必须是编辑或审阅者才能执行此过程。明确地说，您必须具有域的**“列出内容”**和**“读取设置”**权限。
- 若要在请求被批准之前撤销请求，请单击**“挂起”**选项卡。右键单击该 GPO，然后单击**“撤销”**。GPO 将返回到**“非受控”**选项卡。

其他参考

- 创建或控制 GPO

请求创建新的受控 GPO

除非您是审批者或 AGPM 管理员（完全控制），否则您必须请求创建新的 组策略对象 (GPO)。

若要完成此过程，必须使用编辑或审阅者角色的或者拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

使用通过 AGPM 管理的更改控制创建新 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 右键单击**“更改控制”**，然后单击**“新建受控 GPO”**。
3. 除非您有创建 GPO 的特殊权限，否则必须提交创建请求。在**“新建受控 GPO”**对话框中：
   a. 若要接收请求的副本，请在**“抄送”**字段中输入您的电子邮件地址。
   b. 键入新 GPO 的名称。
   c. 可选：键入新 GPO 的注释。
   d. 若要在批准后立即将新 GPO 部署到域的生产环境，请单击**“实时创建”**。若要脱机创建新 GPO 而无须在审批后立即部署，请单击**“脱机创建”**。
   e. 选择用作新 GPO 起始点的 GPO 模板。
   f. 单击**“提交”**。
4. 当“进度”窗口表明总体进度完成时，单击“关闭”。新 GPO 即显示在**“挂起”**选项卡上的 GPO 列表中。当审批者批准您的请求后，GPO 将被移到**“受控”**选项卡。

其他注意事项

- 默认情况下，您必须是编辑或审阅者才能执行此过程。具体而言，您必须拥有域的**“列出内容”**权限。
- 若要在请求被批准之前撤销请求，请单击**“挂起”**选项卡。右键单击该 GPO，然后单击**“撤销”**。该 GPO 将被破坏。

其他参考

- 创建或控制 GPO

从生产中导入 GPO

如果对 高级组策略管理 (AGPM) 之外的受控 组策略对象 (GPO) 进行了更改，则可以从域的生产环境导入 GPO 的副本，然后将其保存在存档中，以使存档和生产环境的状态一致。（要导入一个非受控 GPO，请控制该 GPO。请参阅请求控制非受控 GPO。）

完成此过程需要一个具编辑者、审批者或 AGPM 管理员（完全控制）角色或 AGPM 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

从域的生产环境导入 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击 GPO，然后单击“**从生产导入**”。
4. 键入 GPO 的审计跟踪注释，然后单击“**确定**”。

其他注意事项

- 默认情况下，只有编辑、审批者或者 AGPM 管理员（完全控制），才能执行此过程。明确地说，您必须具有 GPO 的“**列出内容**”和“**编辑设置**”、“**部署 GPO**”或“**删除 GPO**”权限。

其他参考

- 创建或控制 GPO

编辑 GPO

组策略对象 (GPO) 必须为 高级组策略管理 (AGPM) 所控制才能对其进行编辑。有关控制 GPO 的详细信息，请参阅创建或控制 GPO。

若要脱机对 GPO 进行更改而不立即影响生产环境中已部署的 GPO 副本，请从存档中签出 GPO 的副本。更改完成后，将 GPO 签入回存档，对其进行测试，并请求将 GPO 部署到生产环境。

- 脱机编辑 GPO
- 标记 GPO 的当前版本
- 重命名 GPO 或模板

脱机编辑 GPO

要对受控 组策略对象 (GPO) 进行更改，您必须首先从存档中签出 GPO 副本。在将该 GPO 签入之前，其他人无法对其进行修改，从而避免多个组策略管理员的更改相互冲突。修改 GPO 完成后，应将其签入存档，这样可以进行检查并将其部署在生产环境中。

需要使用具有编辑或 AGPM 管理员（完全控制） 角色的用户帐户、创建 GPO 的审批者的用户帐户或者具有 高级组策略管理 (AGPM) 中所需权限的用户帐户，才能完成此过程。请在此主题的“其他考虑事项”中查看详细信息。

脱机编辑 GPO

要编辑 GPO，您应从存档中签出 GPO，脱机对 GPO 进行编辑，然后将 GPO 签入存档，以便对其进行检查和部署（或由其他编辑修改）。

- 从存档中签出 GPO 进行编辑
- 脱机编辑 GPO
- 将 GPO 签入存档

从存档中签出 GPO 进行编辑

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击要编辑的 GPO，然后单击“**签出**”。
4. 键入签出 GPO 时，要在该 GPO 的历史记录中显示的注释，然后单击“**确定**”。
5. 当“**进度**”窗口显示总体进度已完成时，单击“**关闭**”。在“**受控**”选项卡上，GPO 的状态现在标识为“**已签出**”。

脱机编辑 GPO

1. 在“**受控**”选项卡上，右键单击要编辑的 GPO，然后单击“**编辑**”。
2. 在“**组策略管理编辑器**”窗口中，对 GPO 脱机副本进行更改。

   备注

   要禁用所有计算机配置设置或所有用户配置设置，在“**组策略管理编辑器**”窗口中右键单击 GPO，然后单击“**属性**”。根据需要选择“**禁用计算机配置设置**”或“**禁用用户配置设置**”。
3. 修改 GPO 完成后，关闭“**组策略管理编辑器**”窗口。

将 GPO 签入存档

1. 在“**受控**”选项卡上：
   - 如果没有对 GPO 进行更改，则右键单击 GPO 并单击“**撤消签出**”，然后单击“**是**”进行确认。
   - 如果对 GPO 进行了更改，则右键单击 GPO 并单击“**签入**”。
2. 键入将在 GPO 审计跟踪中显示的注释，然后单击“**确定**”。
3. 当“进度”窗口表明总体进度完成时，单击“关闭”。在“**受控**”选项卡上，GPO 状态标识为“**已签入**”。

其他注意事项

- 默认情况下，要签出和编辑 GPO，您必须是创建或控制 GPO 的审批者，即编辑或 AGPM 管理员（完全控制）。具体而言，您必须拥有 GPO 的“**列出内容**”和“**编辑设置**”权限。此外，要编辑 GPO，您必须是签出 GPO 的个人。
- 默认情况下，要签入 GPO，您必须是编辑、审批者或 AGPM 管理员（完全控制）。尤其是，您必须拥有 GPO 的“**列出内容**”和“**编辑设置**”或“**部署 GPO**”权限。如果您不是审批者或 AGPM 管理员（或拥有“**部署 GPO**”权限的其他组策略管理员），您必须是签出 GPO 的编辑。
- 编辑 GPO 时，在其他 GPO 中配置软件包的任何组策略软件安装升级时都会引用部署的 GPO，而不是已签出副本。

其他参考

- 编辑 GPO

- 检查 GPO
    - 检查 GPO 设置
    - 检查 GPO 链接
    - 识别 GPO、GPO 版本或模板之间的差异
- 部署 GPO
    - 请求部署 GPO
    - 部署 GPO

标记 GPO 的当前版本

您可以为当前版本的 组策略对象 (GPO) 添加标记，以便于在其历史记录中进行辨认。可以使用标签对在发生问题时可以回滚的已知正确版本进行标识。另外，如果需要以后进行回滚，那么可以一次使用同一标签对多个 GPO 进行标记，以便对应当回滚到同一点的相关 GPO 进行标记。

完成此过程需要一个具编辑者、审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

在其历史记录中标记当前版本的 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 单击要标记其当前版本的 GPO。要选择多个 GPO，请按住 Shift 并单击相邻一组 GPO 中的最后一个 GPO，或者按住 Ctrl 并单击单个 GPO。右键单击所选 GPO，然后单击“**标签**”。
4. 键入将在每个所选 GPO 的历史记录中显示的标签和注释，然后单击“**确定**”。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。

其他注意事项

- 默认情况下，您必须是编辑者、审批者或 AGPM 管理员（完全控制）才能执行此过程。明确地说，您必须具有 GPO 的“**列出内容**”和“**编辑设置**”或“**部署 GPO**”权限。

其他参考

- 编辑 GPO

重命名 GPO 或模板

您可以重命名受控 组策略对象 (GPO) 或模板。

需要使用具有编辑或 AGPM 管理员（完全控制） 角色的用户帐户、创建 GPO 的审批者的用户帐户或者具有 高级组策略管理 (AGPM) 中所需权限的用户帐户，才能完成此过程。请在此主题的“其他考虑事项”中查看详细信息。

重命名 GPO 或模板

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。

2. 在**“内容”**选项卡上，单击**“受控”**或**“模板”**选项卡，显示要重命名的项目。
3. 右键单击要重命名的 GPO 或模板，然后单击**“重命名”**。
4. 键入 GPO 或模板的新名称和注释，然后单击**“确定”**。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。在**“内容”**选项卡上的新名称下会出现 GPO 或模板。

其他注意事项

- 默认情况下，您必须是创建或控制 GPO 的审批者、编辑或 AGPM 管理员（完全控制），才能执行此过程。明确地说，您必须具有 GPO 的**“列出内容”**和**“编辑设置”**权限。
- 当您重命名已部署的 GPO 时，存档中的名称会立即更改。生产环境中的名称只有在重新部署 GPO 时才会更改。在重新部署 GPO（或删除生产副本）之前，在生产环境中仍使用旧名称，因此该名称不能用于另一个 GPO。同样，在部署 GPO（更改了生产副本的名称）或删除生产副本之前，不能将存档中的 GPO 重命名为其原始名称。

其他参考

- 编辑 GPO

使用测试环境

请求将 组策略对象 (GPO) 部署到生产环境之前，应在实验室环境中对 GPO 进行测试。如果在测试林的域中开发 GPO，则可以将 GPO 导出到文件，再将文件导入生产林中的域。然后可以通过将 GPO 链接到包含测试计算机和用户的组织单位 (OU) 来对 GPO 进行测试。

- 将 GPO 导出到文件
- 从文件中导入 GPO
- 在独立的组织单位中测试 GPO

备注

还可以从域的生产环境导入 GPO。有关详细信息，请参阅从生产中导入 GPO。

将 GPO 导出到文件

可以将受控 组策略对象 (GPO) 导出到 CAB 文件，从而将其复制到其他林中的域，以便将 GPO 导入该域中的 高级组策略管理 (AGPM)。有关如何将 GPO 设置导入新的或现有 GPO 的信息，请参阅从文件中导入 GPO。

完成此过程需要一个具有编辑者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

将 GPO 导出到文件

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击 GPO，然后单击**“导出到”**。
4. 输入要将 GPO 导出到的文件的文件名，然后单击**“导出”**。如果该文件不存在，则将进行创

建。如果该文件已存在，则将进行替换。

其他注意事项

- 默认情况下，必须是编辑者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有 GPO 的**“列出内容”**、**“读取设置”**和**“导出 GPO”**权限。

其他参考

- 使用测试环境

从文件中导入 GPO

在 高级组策略管理 (AGPM) 中，如果已将 组策略对象 (GPO) 导出到 CAB 文件，则可以将该 GPO 的策略设置导入其他林的域中的现有 GPO。将策略设置导入现有 GPO 将替换该 GPO 中的所有策略设置。有关将 GPO 设置导出到 CAB 文件的信息，请参阅将 GPO 导出到文件。

完成此过程需要一个具有编辑者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

将策略设置导入现有 GPO

1. 在**“组策略管理控制台”**树中，单击要将策略设置导入的域中的**“更改控制”**。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 签出要将策略设置导入的目标 GPO。
4. 右键单击目标 GPO，指向**“导入自”**，然后单击**“文件”**。
5. 按照**“导入设置向导”**中的说明选择 GPO 备份，导入其策略设置以替换目标 GPO 中的策略设置，然后输入目标 GPO 的审计跟踪的注释。默认情况下，向导完成后将签入目标 GPO。

其他注意事项

- 默认情况下，必须是编辑者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有域的**“列出内容”**、**“编辑设置”**和**“导入 GPO”**权限，且该 GPO 必须由您签出。
- 尽管编辑在创建新 GPO 时无法将策略设置导入该 GPO 中，但编辑可以请求创建新 GPO，然后在创建后将策略设置导入其中。

其他参考

- 使用测试环境

在独立的组织单位中测试 GPO

如果在生产环境中进行部署之前，在同一域中使用测试组织单位 (OU) 测试 组策略对象 (GPO)，则必须拥有访问测试 OU 所需的权限。使用测试 OU 是可选的。

使用测试 OU

1. 尽管您已签出 GPO 进行编辑，但可以在**“组策略管理控制台”**中，单击要在其中管理 GPO 的林和域中的**“组策略对象”**。
2. 单击要测试的已签出 GPO 的副本。名称之前会有**“[AGPM]”**字样。（如果未列出，请单击“

操作”，然后单击**“刷新”**。按字母顺序对名称排序，**“[AGPM]”**GPO 通常出现在列表顶部。）

3. 将 GPO 拖到测试 OU。
4. 在询问是否创建指向测试 OU 中 GPO 的链接的对话框中，单击**“确定”**。

其他注意事项

- 测试完成时，签入 GPO 会自动删除指向已签出 GPO 副本的链接。

其他参考

- 使用测试环境

请求部署 GPO

在修改并签入 组策略对象 (GPO) 后，部署 GPO，以使其在生产环境中生效。

若要完成此过程，必须使用编辑角色的或拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

请求将 GPO 部署到域的生产环境

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击要部署的 GPO，然后单击**“部署”**。
4. 除非您是审批者或 AGPM 管理员，或者拥有部署 GPO 的特殊权限，否则必须提交部署请求。若要接收请求的副本，请在**“抄送”**字段中键入您的电子邮件地址。键入要在 GPO 的**“历史记录”**中显示的注释，然后单击**“提交”**。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。GPO 即显示在**“挂起”**选项卡上的 GPO 列表中。当审批者批准您的请求后，GPO 将从**“挂起”**选项卡移到**“受控”**选项卡，并得以部署。

其他注意事项

- 默认情况下，您必须是编辑才能执行此过程。具体而言，您必须拥有 GPO 的**“列出内容”**和**“编辑设置”**权限。
- 若要在请求被批准之前撤销请求，请单击**“挂起”**选项卡。右键单击该 GPO，然后单击**“撤销”**。GPO 将返回到**“受控”**选项卡。

其他参考

- 执行编辑任务

创建模板和设置默认模板

创建模板允许您保存特定版本 组策略对象 (GPO) 的所有设置，并将这些设置用作创建新 GPO 的起点。作为编辑，您还可以指定哪个可用模板将是所有组策略管理员创建新 GPO 时使用的默认模板。

模板的一些可能使用方法包括：

- 创建组织可以跨域重新使用的安全基准。
- 创建一个模板，用于管理文件夹重定向以及组织可以为每个部门自定义的脱机文件。
- 创建无线网络模板，组织可以用来为不同地理区域配置无线网络连接。
- 为本地网络管理员创建法规遵从模板。
- 创建现有 GPO 的只读快照。

备注

模板是 GPO 的静态版本，无法进行编辑，但可用作创建新的可编辑 GPO 的起点。重命名或删除模板不会影响创建自该模板的 GPO。

- 创建模板
- 设置默认模板

创建模板

创建模板使您能够保存特定版本 组策略对象 (GPO) 的所有设置，并将这些设置用作创建新 GPO 的起点。

备注

模板是 GPO 的静态、不可编辑版本，可用作创建新的可编辑 GPO 的起始点。

完成此过程需要一个具有编辑者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的"其他考虑事项"中查看详细信息。

基于现有 GPO 创建模板

1. 在"**组策略管理控制台**"树中，单击您要在其中管理 GPO 的林和域中的"**更改控制**"。
2. 在详细信息窗格中的"**内容**"选项卡上，单击"**受控**"或"**非受控**"选项卡，以显示可用 GPO。
3. 右键单击要从中创建模板的 GPO，然后单击"**另存为模板**"。
4. 键入模板名称和注释，然后单击"**确定**"。
5. 当"进度"窗口表明总体进度完成时，单击"关闭"。新模板会出现在"**模板**"选项卡上。

其他注意事项

- 默认情况下，您必须是编辑或 AGPM 管理员（完全控制） 才能执行此过程。具体而言，您必须拥有域的"**列出内容**"和"**创建模板**"权限。
- 重命名或删除模板不会影响基于该模板创建的 GPO。
- 因为模板无法改变，所以模板没有历史记录。

其他参考

- 创建模板和设置默认模板
- 请求创建新的受控 GPO

设置默认模板

作为编辑，您可以指定将哪些可用模板作为建议所有组策略管理员在创建新 组策略对象 (GPO) 时使用的默认模板。

备注

模板是 GPO 的静态、不可编辑版本，可用作创建新的可编辑 GPO 的起始点。

完成此过程需要一个具有编辑者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

设置创建新 GPO 时使用的默认模板

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格的“**内容**”选项卡上，单击“**模板**”选项卡以显示可用的模板。
3. 右键单击要设置为默认模板的模板，然后单击“**设为默认值**”。
4. 单击“**是**”确认。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。默认模板有蓝色图标，并且其在“**模板**”选项卡上的状态标识为“**模板(默认)**”。

其他注意事项

- 默认情况下，您必须是编辑或 AGPM 管理员（完全控制） 才能执行此过程。具体而言，您必须拥有域的“**列出内容**”和“**创建模板**”权限。
- 在将某个模板设置为默认模板后，该模板将是组策略管理员在创建新 GPO 时最初在“**新建受控 GPO**”对话框中选定的模板。但是，这些管理员可以选择任何其他 GPO 模板，包括其中不包含任何设置的“**<空 GPO>**”。
- 重命名或删除模板不会影响基于该模板创建的 GPO。
- 因为模板无法改变，所以模板没有历史记录。

其他参考

- 创建模板和设置默认模板
- 请求创建新的受控 GPO

删除或还原 GPO

要使用 高级组策略管理 (AGPM) 从存档中删除 组策略对象 (GPO) 或从回收站还原删除的 GPO，GPO 必须受控于 AGPM。作为编辑，您可能没有完成删除或还原 GPO 操作的权限，但是您具有开始该过程并向审批者提交请求所需的权限。

- 请求删除 GPO
- 请求还原已删除的 GPO

请求删除 GPO

除非您是审批者或 AGPM 管理员（完全控制），否则必须请求删除 组策略对象 (GPO)。

若要完成此过程，必须使用编辑角色的或拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

请求删除受控 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击要删除的 GPO，然后单击**“删除”**。
    - 要从存档中删除 GPO，而不改变生产环境中的 GPO 部署版本，请单击**“仅从存档中删除 GPO”**。
    - 要同时从存档和域的生产环境中删除 GPO，请单击**“从存档和生产中删除 GPO”**。
4. 除非您拥有删除 GPO 的特殊权限，否则必须提交删除部署 GPO 的请求。若要接收请求的副本，请在**“抄送”**字段中键入您的电子邮件地址。键入在 GPO 审计跟踪中要显示的注释，然后单击**“提交”**。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。GPO 即显示在**“挂起”**选项卡上的 GPO 列表中。审批者批准您的请求后，GPO 会从**“挂起”**选项卡移到**“回收站”**选项卡，在此处可以还原或毁坏它。

其他注意事项

- 默认情况下，您必须是编辑才能执行此过程。具体而言，您必须拥有 GPO 的**“列出内容”**和**“编辑设置”**权限。
- 若要在请求被批准之前撤销请求，请单击**“挂起”**选项卡。右键单击该 GPO，然后单击**“撤销”**。GPO 将返回到**“受控”**选项卡。
- 要从生产环境中删除非受控 GPO 而不是先控制它，请在**“组策略管理控制台”**中，单击**“林”**，单击**“域”**，单击 <**MyDomain**>，然后单击**“组策略对象”**。右键单击非受控 GPO，然后单击**“删除”**。

其他参考

- 删除或还原 GPO

请求还原已删除的 GPO

除非您是审批者或 AGPM 管理员（完全控制），否则您必须请求从回收站还原删除的 组策略对象 (GPO)，才能将其返回到存档中。

若要完成此过程，必须使用编辑角色的或拥有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

请求还原删除的 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在**“内容”**选项卡上，单击**“回收站”**选项卡以显示已删除的 GPO。
3. 右键单击要还原的 GPO，然后单击**“还原”**。
4. 除非您拥有还原 GPO 的特殊权限，否则必须提交请求来还原删除的 GPO。若要接收请求的

副本，请在**“抄送”**字段中键入您的电子邮件地址。键入在 GPO 审计跟踪中要显示的注释，然后单击**“提交”**。

5. 当“进度”窗口表明总体进度完成时，单击“关闭”。GPO 即从**“回收站”**选项卡中删除，并显示在**“受控”**选项卡上。

> **备注**
> 如果已从生产环境中删除某个 GPO，则将该 GPO 还原到存档不会自动将其重新部署到生产环境。若要将 GPO 返回到生产环境，请部署 GPO。有关信息，请参阅请求部署 GPO。

其他注意事项

- 默认情况下，您必须是编辑才能执行此过程。明确地说，您必须具有 GPO 的**“列出内容”**和**“编辑设置”**权限。
- 若要在请求被批准之前撤销请求，请单击**“挂起”**选项卡。右键单击该 GPO，然后单击**“撤销”**。GPO 将返回到**“回收站”**选项卡。

其他参考

- 删除或还原 GPO

执行审批者任务

审批者是由 AGPM 管理员（完全控制） 授权创建、部署和删除 组策略对象 (GPO) 以及批准或拒绝（通常来自编辑的）创建、部署或删除 GPO 请求的人员。

> **重要事项**
> 确保您已连接到 GPO 的中央存档。有关详细信息，请参阅配置 AGPM 服务器连接。

- 批准或拒绝挂起的操作
- 创建或控制 GPO
- 签入 GPO
- 部署 GPO
- 回滚到早期版本的 GPO
- 删除、还原或破坏 GPO

> **备注**
> 批准 GPO 之前，审批者应检查其中包含的策略设置。审批者角色包括审阅者角色的权限，因此审批者可以查看策略设置和比较 GPO。有关详细信息，请参阅执行审阅者任务。

其他注意事项

默认情况下，为审批者角色提供了下列权限：

- 列出内容
- 读取设置

- 创建 GPO
- 部署 GPO
- 删除 GPO

此外，审批者对自己创建或控制的 GPO 有完全控制权限。

批准或拒绝挂起的操作

审批者的核心职责是评估后批准或拒绝编辑或审阅者创建、部署和删除 组策略对象 (GPO) 的请求，后二者不具备完成这些操作的权限。报告可以帮助审批者评估 GPO 的新版本。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的"其他考虑事项"中查看详细信息。

批准或拒绝挂起的请求

1. 在"**组策略管理控制台**"树中，单击您要在其中管理 GPO 的林和域中的"**更改控制**"。
2. 在"**内容**"选项卡上，单击"**挂起**"选项卡以显示挂起的 GPO。
3. 右键单击挂起的 GPO，然后单击"**批准**"或"**拒绝**"。
4. 如果批准部署，请单击"**批准挂起操作**"对话框上的"**高级**"以查看指向 GPO 的链接。将鼠标指针暂停在树中的项目上会显示详细信息。
    - 默认情况下，将还原所有指向 GPO 的链接。
    - 若要防止还原链接，请清除该链接的复选框。
    - 若要防止还原所有链接，请清除"**部署 GPO**"对话框中的"**还原链接**"复选框。
5. 单击"**是**"或"**确定**"确认批准或拒绝挂起的操作。如果您已批准请求，GPO 即会移到与所执行的操作对应的选项卡。

    备注

    如果审批者的电子邮件地址包含在"**域委托**"选项卡上的"**收件人电子邮件地址**"字段中，则当编辑或审阅者提交请求时，审批者将收到一封从 AGPM 别名发来的电子邮件。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有执行审批请求所需的权限。

其他参考

- 执行审批者任务

创建或控制 GPO

要使用 高级组策略管理 (AGPM) 提供 组策略对象 (GPO) 更改控制，您必须首先使用 AGPM 控制 GPO。在"**更改控制**"文件夹中创建的新 GPO 将自动成为受控 GPO。

- 控制非受控 GPO

- 创建新的受控 GPO
- 委派管理受控 GPO
- 从生产中导入 GPO

控制非受控 GPO

若要提供对 组策略对象 (GPO) 的更改控制，必须先控制 GPO。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的"其他考虑事项"中查看详细信息。

控制非受控 GPO

1. 在"**组策略管理控制台**"树中，单击您要在其中管理 GPO 的林和域中的"**更改控制**"。
2. 在详细信息窗格的**"内容"**选项卡上，单击**"非受控"**选项卡以显示非受控 GPO。
3. 右键单击要使用 AGPM 控制的 GPO，然后单击**"控制"**。
4. 键入要在 GPO 的历史记录中显示的注释，然后单击**"确定"**。
5. 当"进度"窗口表明总体进度完成时，单击"关闭"。GPO 即从**"非受控"**选项卡的列表中删除并被添加到**"受控"**选项卡上。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有域的**"列出内容"**和**"创建 GPO"**权限。

其他参考

- 创建或控制 GPO

创建新的受控 GPO

在**"更改控制"**文件夹中创建的新 组策略对象 (GPO) 将自动成为受控 gpo，因而可以进行管理。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的"其他考虑事项"中查看详细信息。

使用通过 AGPM 管理的更改控制创建新 GPO

1. 在"**组策略管理控制台**"树中，单击您要在其中管理 GPO 的林和域中的"**更改控制**"。
2. 右键单击**"更改控制"**，然后单击**"新建受控 GPO"**。
3. 在**"新建受控 GPO"**对话框中：
   a. 键入新 GPO 的名称。
   b. 可选：键入将在新 GPO 的**"历史记录"**中显示的新 GPO 的注释。
   c. 要立即将新 GPO 部署到域的生产环境，请单击**"实时创建"**。要脱机创建新 GPO 而不立即部署它，请单击**"脱机创建"**。
   d. 选择要用作新 GPO 的起点的 GPO 模板，然后单击**"确定"**。

4. 当“进度”窗口表明总体进度完成时，单击“关闭”。新 GPO 会显示在**“受控”**选项卡的 GPO 列表中。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有域的**“列出内容”**和**“创建 GPO”**权限。

其他参考

- 创建或控制 GPO

委派管理受控 GPO

审批者可以委派管理由其创建的受控 组策略对象 (GPO)。像 AGPM 管理员（完全控制） 一样，审批者可以委派对这种 GPO 的访问权限，以便所选编辑可以编辑它，审阅者可以检查它，其他审批者可以批准它。默认情况下，审批者不能委派由另一组策略管理员创建的 GPO 的访问权限。

若要完成此过程，必须使用具有 AGPM 管理员（完全控制） 角色的用户帐户、创建 GPO 的审批者的用户帐户，或者具有 高级组策略管理 (AGPM) 中必需权限的用户帐户。请在此主题的“其他考虑事项”中查看详细信息。

委托受控 GPO 的管理

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格的**“内容”**选项卡上，单击**“受控”**选项卡以显示受控 GPO，然后单击 GPO 进行委托：
   a. 若要为用户或组添加访问权限，请单击**“添加”**按钮，选择相应用户或组，然后单击**“确定”**。在**“添加组或用户”**对话框中，选择角色并单击**“确定”**。
   b. 要删除用户或组的访问权限，请选择该用户或组，然后单击**“删除”**按钮。

      备注

      如果用户或组继承域范围内的访问权限，则**“删除”**按钮不可用。可以在**“域委托”**选项卡上修改域范围内的访问权限。

   c. 若要修改委托给用户或组的角色和权限，请单击**“高级”**按钮。在**“权限”**对话框中，选择用户或组，选中要分配给该用户或组的每个角色对应的复选框，然后单击**“确定”**。

      备注

      编辑和审批者的权限包括审阅者的权限。

其他注意事项

- 默认情况下，您必须是创建或控制 GPO 的审批者或 AGPM 管理员（完全控制） 才能执行此过程。具体而言，您必须拥有域的**“列出内容”**权限和 GPO 的**“修改安全性”**权限。
- 若要将读取访问权限委托给使用 AGPM 的组策略管理员，则必须授予他们**“列出内容”**及**“读取设置”**权限。他们使用该权限可以查看 AGPM 的**“内容”**选项卡上的 GPO。其他权限必须明确委托。
- 编辑必须拥有已部署 GPO 副本的**“读取”**权限，才能充分利用组策略软件安装。

其他参考

- 创建或控制 GPO

从生产中导入 GPO

如果对 高级组策略管理 (AGPM) 之外的受控 组策略对象 (GPO) 进行了更改，则可以从域的生产环境导入 GPO 的副本，然后将其保存在存档中，以使存档和生产环境的状态一致。（要导入一个非受控 GPO，请控制该 GPO。请参阅控制非受控 GPO。）

完成此过程需要一个具编辑者、审批者或 AGPM 管理员（完全控制）角色或 AGPM 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

从域的生产环境导入 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击 GPO，然后单击“**从生产导入**”。
4. 键入 GPO 的审计跟踪注释，然后单击“**确定**”。

其他注意事项

- 默认情况下，只有编辑、审批者或者 AGPM 管理员（完全控制），才能执行此过程。明确地说，您必须具有 GPO 的“**列出内容**”和“**编辑设置**”、“**部署 GPO**”或“**删除 GPO**”权限。

其他参考

- 创建或控制 GPO

签入 GPO

通常，编辑应当在其修改完成时签入他们编辑的 组策略对象 (GPO)。（有关详细信息，请参阅脱机编辑 GPO。）但是，当编辑没有空时，审批者也可以签入 GPO。

完成此过程需要一个具编辑者、审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

签入编辑签出的 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
   - 要放弃编辑所做的更改，请右键单击 GPO，单击“**撤消签出**”，然后单击“**是**”进行确认。
   - 要保留编辑所做的更改，请右键单击 GPO，然后单击“**签入**”。
3. 键入将在 GPO 审计跟踪中显示的注释，然后单击“**确定**”。
4. 当“进度”窗口表明总体进度完成时，单击“关闭”。在“**受控**”选项卡上，GPO 状态标识为“**已签入**”。

其他注意事项

- 默认情况下，您必须是编辑者、审批者或 AGPM 管理员（完全控制）才能执行此过程。明确地说，您必须具有 GPO 的**“列出内容”**和**“编辑设置”**或**“部署 GPO”**权限。如果您不是审批者或 AGPM 管理员（或具有**“部署 GPO”**权限的其他组策略管理员），则必须是签出 GPO 的编辑。

其他参考

- 执行审批者任务
- 脱机编辑 GPO

部署 GPO

审批者可以将新的或已编辑的 组策略对象 (GPO) 部署到生产环境中。有关重新部署早期版本的 GPO 的信息，请参阅回滚到早期版本的 GPO。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

在生产环境中部署 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击要部署的 GPO，然后单击**“部署”**。
4. 要检查 GPO 的链接，请单击**“高级”**。将鼠标指针暂停在树中的项目上会显示详细信息。
   - 默认情况下，将还原所有指向 GPO 的链接。
   - 若要防止还原链接，请清除该链接的复选框。
   - 若要防止还原所有链接，请清除**“部署 GPO”**对话框中的**“还原链接”**复选框。
5. 单击**“是”**。当“进度”窗口表明总体进度完成时，单击“关闭”。

备注

要验证是否已部署最新版本 GPO，请在**“受控”**选项卡上双击要显示其**“历史记录”**的 GPO。GPO 的**“历史记录”**中的**“状态”**列指示是否已部署 GPO。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有 GPO 的**“列出内容”**和**“部署 GPO”**权限。

其他参考

- 执行审批者任务

回滚到早期版本的 GPO

审批者可以通过重新部署 GPO 历史记录中 GPO 的早期版本将更改更回滚到 组策略对象 (GPO)。部署 GPO 的早期版本将覆盖当前生产中的 GPO 版本。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

将 GPO 的早期版本部署到域的生产环境

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 双击要部署的 GPO 以显示其“**历史记录**”。
4. 右键单击要部署的版本，单击“**部署**”，然后单击“**是**”。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。在“**历史记录**”窗口中，单击“**关闭**”。

备注

若要验证已重新部署的版本是否与所需的版本匹配，请检查这两个版本的差异报告。在 GPO 的“**历史记录**”窗口中，突出显示这两个版本，单击右键并选择“**差异**”，然后再选择“**HTML 报告**”或“**XML 报告**”。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有 GPO 的“**列出内容**”和“**部署 GPO**”权限。

其他参考

- 执行审批者任务

删除、还原或破坏 GPO

作为一个审批者，您可以删除 组策略对象 (GPO)（将它移到回收站），从回收站还原 GPO（使它返回存档），也可以破坏 GPO（永久删除它，这样不可以再还原它）。

- 删除受控 GPO
- 还原已删除的 GPO
- 破坏 GPO

删除受控 GPO

审批者可以删除受控 组策略对象 (GPO)，将它移到回收站。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

删除受控 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**控制的**”选项卡以显示控制的 GPO。
3. 右键单击要删除的 GPO，然后单击“**删除**”。
   - 要从存档中删除 GPO，而不改变生产环境中的 GPO 部署版本，请单击“**仅从存档中删除 GPO**”。
   - 要同时从存档和域的生产环境中删除 GPO，请单击“**从存档和生产中删除 GPO**”。

4. 键入将在 GPO 审核跟踪中显示的注释，然后单击**“确定”**。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。GPO 已从**“受控”**选项卡上删除，而且显示在**“回收站”**选项卡上，在此处可以还原或破坏 GPO。如果仅从存档中删除 GPO，它还会显示在**“非受控”**选项卡上。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有 GPO 的**“列出内容”**和**“删除 GPO”**权限。
- 要从生产环境中删除非受控 GPO 而不是先控制它，请在**“组策略管理控制台”**中，单击**“林”**，单击**“域”**，单击 **<MyDomain>**，然后单击**“组策略对象”**。右键单击非受控 GPO，然后单击**“删除”**。

其他参考

- 删除、还原或破坏 GPO

还原已删除的 GPO

审批者可以从回收站中还原已删除的 组策略对象 (GPO)，将其返回到存档。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

还原已删除的 GPO

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在**“内容”**选项卡上，单击**“回收站”**选项卡以显示已删除的 GPO。
3. 右键单击要还原的 GPO，然后单击**“还原”**。
4. 键入要在 GPO 的历史记录中显示的注释，然后单击**“确定”**。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。GPO 即从**“回收站”**选项卡中删除，并显示在**“受控”**选项卡上。

备注

如果已从生产环境中删除某个 GPO，则将该 GPO 还原到存档不会自动将其重新部署到生产环境。若要将 GPO 返回到生产环境，请部署 GPO。有关信息，请参阅部署 GPO。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有 GPO 的**“列出内容”**及**“部署 GPO”**或**“删除 GPO”**权限。

其他参考

- 删除、还原或破坏 GPO

破坏 GPO

审批者可以破坏 组策略对象 (GPO)，即从回收站中将其删除，从而将其永久删除，以使其永远不可再还原。

完成此过程需要一个具有审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

永久删除 GPO，以使其永远不可再还原

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在“**内容**”选项卡上，单击“**回收站**”选项卡以显示已删除的 GPO。
3. 右键单击要破坏的 GPO，然后单击“**破坏**”。
4. 单击“**是**”确认您要从存档中永久删除选定的 GPO 和所有备份。
5. 当“进度”窗口表明总体进度完成时，单击“关闭”。GPO 即从“**回收站**”选项卡中删除，从而永久删除。

其他注意事项

- 默认情况下，您必须是审批者或 AGPM 管理员（完全控制）才能执行此过程。具体而言，您必须拥有 GPO 的“**列出内容**”和“**删除 GPO**”权限。

其他参考

- 删除、还原或破坏 GPO

执行审阅者任务

审阅者是 AGPM 管理员（完全控制） 授权审阅或审核 组策略对象 (GPO) 的人员。仅具有审阅者角色的个人无法修改 GPO，但是，所有其他角色都包括审阅者角色。

- 配置 AGPM 服务器连接
- 检查 GPO 设置
- 检查 GPO 链接
- 识别 GPO、GPO 版本或模板之间的差异

其他注意事项

默认情况下，为审阅者角色提供下列权限：

- 列出内容
- 读取设置

配置 AGPM 服务器连接

要确保您已连接到正确的中央存档，请检查 AGPM 服务器连接的配置。如果 AGPM 管理员（完全控制） 没有为您配置 AGPM 服务器连接，您必须手动配置它。

选择 AGPM 服务器

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中，单击“**AGPM 服务器**”选项卡：

- 如果**“AGPM 服务器”**选项卡上的选项不可用，那么这些选项已由 AGPM 管理员进行了集中配置。
- 如果**“AGPM 服务器”**选项卡上的选项可用，请键入 AGPM 服务器的完全限定计算机名称（例如，server.contoso.com）和 AGPM 服务监听的端口（默认情况下，为端口 4600）。单击**“应用”**，然后单击**“是”**进行确认。

其他注意事项

- 所选 AGPM 服务器确定在**“内容”**选项卡显示的 GPO，以及**“域委托”**选项卡设置应用的位置。如果不通过管理模板进行集中管理，则每个组策略管理员必须配置此设置，才能指向域的 AGPM 服务器。

其他参考

- 执行审阅者任务

检查 GPO 设置

您可以生成基于 HTML 或基于 XML 的报告，以检查任何 组策略对象 (GPO) 版本中的设置。

完成此过程需要一个具有审阅者、编辑者、审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

检查任何 GPO 版本中的设置

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中的**“内容”**选项卡上，单击一个选项卡以显示 GPO。
3. 双击 GPO 显示其历史记录。
4. 右键单击要检查其设置的 GPO 版本，单击**“设置”**，然后单击**“HTML 报告”**或**“XML 报告”**，以显示 GPO 设置的摘要。

其他注意事项

- 默认情况下，您必须是审阅者、编辑者、审批者或 AGPM 管理员（完全控制）才能执行此过程。特别是，您必须对 GPO 具有“**列出内容**”和“**读取设置**”权限。此外，要显示 GPO 列表，您必须对域具有“**列出内容**”权限。

其他参考

- 执行审阅者任务

检查 GPO 链接

您可以显示一个图表，显示选择链接到组织单位的一个或多个 组策略对象 (GPO)。每次控制、导入或签入 GPO 时都会更新 GPO 链接图表。

完成此过程需要一个具有审阅者、编辑者、审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

检查 GPO 链接

- 对于一个或多个 GPO
- 对于一个或多个版本的 GPO

显示一个或多个 GPO 的 GPO 链接

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中的**“内容”**选项卡上，单击**“受控”**、**“挂起”**或**“回收站”**选项卡，以显示 GPO。
3. 选择一个或多个要显示其链接的 GPO，右键单击所选 GPO，单击**“设置”**，然后单击**“GPO 链接”**，以显示包含所选 GPO 链接的域和组织单位的图表。

显示一个或多个版本的 GPO 的 GPO 链接

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中的**“内容”**选项卡上，单击**“受控”**或**“回收站”**选项卡，以显示 GPO。
3. 双击 GPO 显示其历史记录。
4. 右键单击要检查其设置的 GPO 版本，单击**“设置”**，然后单击**“HTML 报告”**或**“XML 报告”**，以显示 GPO 设置的摘要。

其他注意事项

- 默认情况下，您必须是审阅者、编辑者、审批者或 AGPM 管理员（完全控制）才能执行此过程。特别是，您必须对 GPO 具有“**列出内容**”和“**读取设置**”权限。此外，要显示 GPO 列表，您必须对域具有“**列出内容**”权限。

其他参考

- 执行审阅者任务

识别 GPO、GPO 版本或模板之间的差异

您可以通过生成基于 HTML 或基于 XML 的差异报告，分析 组策略对象 (GPO)、模板或不同版本 GPO 之间的差异。

完成此过程需要一个具有审阅者、编辑者、审批者或 AGPM 管理员（完全控制）角色或高级组策略管理 (AGPM) 中的必要权限的用户帐户。 请在此主题的“其他考虑事项”中查看详细信息。

识别 GPO、GPO 版本或模板之间的差异

- 两个 GPO 或两个模板之间的差异
- GPO 与模板之间的差异
- 同一 GPO 的两个版本之间的差异
- GPO 版本与模板之间的差异

识别两个 GPO 或两个模板之间的差异

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中的“**内容**”选项卡上，单击一个选项卡以显示 GPO（或模板，如果比较两个模板的话）。
3. 选择两个 GPO 或两个模板。
4. 右键单击其中一个 GPO 或模板，单击“**差异**”，然后单击“**HTML 报告**”或“**XML 报告**”，以显示包含 GPO 或模板的设置摘要的差异报告。

识别 GPO 与模板之间的差异

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中的“**内容**”选项卡上，单击一个选项卡以显示 GPO（或模板，如果比较两个模板的话）。
3. 右键单击 GPO，单击“**差异**”，然后单击“**模板**”。
4. 选择模板和报告类型，然后单击“**确定**”，以显示包含 GPO 和模板的设置摘要的差异报告。

识别同一 GPO 的两个版本之间的差异

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中的“**内容**”选项卡上，单击一个选项卡以显示 GPO（或模板，如果比较两个模板的话）。
3. 双击 GPO 显示其历史记录，然后突出显示要比较的版本。
4. 右键单击其中一个版本，单击“**差异**”，然后单击“**HTML 报告**”或“**XML 报告**”，以显示包含 GPO 的设置摘要的差异报告。

识别 GPO 版本与模板之间的差异

1. 在“**组策略管理控制台**”树中，单击您要在其中管理 GPO 的林和域中的“**更改控制**”。
2. 在详细信息窗格中的“**内容**”选项卡上，单击一个选项卡以显示 GPO（或模板，如果比较两个模板的话）。
3. 双击 GPO 显示其历史记录。
4. 右键单击感兴趣的 GPO 版本，单击“**差异**”，然后单击“**模板**”。
5. 选择模板和报告类型，然后单击“**确定**”，以显示包含 GPO 版本和模板的设置摘要的差异报告。

差异报告中的关键字

符号	意义	颜色
无	同时存在于两个 GPO 中，具有	随级别变化

符号	意义	颜色
	相同设置的项目	
[#]	同时存在于两个 GPO 中，但具有不同的设置的项目	蓝色
[-]	仅存在于第一个 GPO 中的项目	红色
[+]	仅存在于第二个 GPO 中的项目	绿色

- 对于具有不同设置的项目来说，当展开项目时会标识出不同设置。在每个 GPO 中显示属性值的顺序与在报告中显示 GPO 的顺序相同。
- 当对设置进行某些更改后，可能会导致将一个项目报告为两个不同项目（一个仅存在于第一个 GPO 中，另一个仅存在于第二个 GPO 中），而不是报告为一个已更改项目。

其他注意事项

- 默认情况下，您必须是审阅者、编辑者、审批者或 AGPM 管理员（完全控制）才能执行此过程。特别是，您必须对 GPO 具有“**列出内容**”和“**读取设置**”权限。此外，要显示 GPO 列表，您必须对域具有“**列出内容**”权限。

其他参考

- 执行审阅者任务

AGPM 疑难解答

本部分列出了在使用 高级组策略管理 (AGPM) 管理 组策略对象 (GPO) 时遇到的一些常见问题。若要诊断此处未列出的问题，使用日志记录和跟踪对于 AGPM 管理员（完全控制） 可能很有帮助。有关详细信息，请参阅配置日志记录和跟踪。

注意

- 有关在出现问题时回滚到早期版本的 GPO 的信息，请参阅回滚到早期版本的 GPO。
- 有关如何通过从备份还原完整存档来从灾难中恢复的信息，请参阅从备份中还原存档。

您遇到了什么问题？

- 我无法访问存档
- GPO 状态因组策略管理员不同而有所不同
- 我无法修改 AGPM 服务器连接
- 我无法更改默认模板或无法查看、创建、编辑、重命名、部署或删除 GPO
- 我无法使用特定 GPO 名称
- 我未收到 AGPM 电子邮件通知
- AGPM 服务无法使用端口 4600
- AGPM 服务将不启动

- 组策略软件安装无法安装软件
- 将存档还原到新 AGPM 服务器时发生错误

我无法访问存档

- **原因**：您没有为存档选择正确的服务器和端口。
- **解决方案**：
  - 如果您是 AGPM 管理员：请参阅配置 AGPM 服务器连接。
  - 如果您不是 AGPM 管理员：从 AGPM 管理员 请求 AGPM 服务器的连接详细信息。请参阅配置 AGPM 服务器连接。
- **原因**：AGPM 服务未运行。
- **解决方案**：
  - 如果您是 AGPM 管理员：启动 AGPM 服务。有关详细信息，请参阅启动和停止 AGPM 服务。
  - 如果您不是 AGPM 管理员：联系 AGPM 管理员 以获取帮助。

GPO 状态因组策略管理员不同而有所不同

- **原因**：不同的组策略管理员为同一存档选择了不同的 AGPM 服务器。
- **解决方案**：
  - 如果您是 AGPM 管理员：请参阅配置 AGPM 服务器连接。
  - 如果您不是 AGPM 管理员：从 AGPM 管理员 请求 AGPM 服务器的连接详细信息。请参阅配置 AGPM 服务器连接。

我无法修改 AGPM 服务器连接

- **原因**：如果“**AGPM 服务器**”选项卡上的设置不可用，则已使用管理模板在中央配置了 AGPM 服务器。
- **解决方案**：
  - 如果您是 AGPM 管理员：如果“**AGPM 服务器**”选项卡上的设置不可用，请参阅配置 AGPM 服务器连接。
  - 如果您不是 AGPM 管理员：如果“**AGPM 服务器**”选项卡上的设置不可用，您不需要修改 AGPM 服务器。

我无法更改默认模板或无法查看、创建、编辑、重命名、部署或删除 GPO

- **原因**：您未被分配执行一个或多个任务所需权限的角色。
- **解决方案**：
  - 如果您是 AGPM 管理员：请参阅委派对存档的域级别访问权限和委派对存档中单个 GPO 的访问权限。AGPM 权限将通过级联方式从域传递到当前存档中存在的所有 GPO。有关可执行任务的角色及执行任务所需权限的详细信息，请参阅该任务的帮助。
  - 如果您不是 AGPM 管理员，则需要其他的角色或权限：联系 AGPM 管理员 以获取帮助。请注意，如果您是编辑，则可以开始在域的生产环境中执行创建 GPO、部署 GPO 或删除 GPO 的过程，但是审批者或 AGPM 管理员 必须批准了您的请求。

我无法使用特定 GPO 名称

- **原因**：GPO 名称已在使用中或者您没有列出 GPO 的权限。
- **解决方案**：
  - 如果 GPO 名称出现在**“受控”**、**“非受控”**或者**“挂起”**选项卡上，请选择其他名称。如果部署的 GPO 已被重命名但尚未重新部署，该 GPO 将以其旧名称显示在域的生产环境中。因此，仍使用旧名称。重新部署 GPO 以在生产环境中更新其名称，然后释放该名称，以便其他 GPO 使用该名称。
  - 如果 GPO 名称没有出现在**“受控”**、**“非受控”**或**“挂起”**选项卡上，则表示您可能没有列出 GPO 的权限。要请求权限，请联系 AGPM 管理员。

我未收到 AGPM 电子邮件通知

- **原因**：尚未提供有效 SMTP 电子邮件服务器和电子邮件地址，或者没有进行生成电子邮件通知的任何操作。
- **解决方案**：
  - 如果您是 AGPM 管理员：对于由 AGPM 发送的关于挂起操作的电子邮件通知，AGPM 管理员必须在**“域委托”**选项卡上为审批者提供有效的 SMTP 电子邮件服务器和电子邮件地址。有关详细信息，请参阅配置电子邮件通知。
  - 只有当编辑、审阅者或者其他组策略管理员（他们不具有创建、部署或者删除 GPO 所需的权限）提交一个请求而发生任何一种操作时，才会生成电子邮件通知。没有批准或拒绝请求的自动通知。

AGPM 服务无法使用端口 4600

- **原因**：默认情况下，AGPM 服务监听的端口是 4600。
- **解决方案**：如果端口 4600 不可用于 AGPM 服务，请修改 AGPM 服务器的端口配置以使用其他端口，然后更新 AGPM 客户端 AGPM 服务器连接中的端口。有关详细信息，请参阅修改 AGPM 服务。

AGPM 服务将不启动

- **原因**：您已在操作系统中修改了**“管理工具”**和**“服务”**下的 AGPM 服务设置。
- **解决方案**：在“控制面板”中修改**“程序和功能”**下的“Microsoft Advanced Group Policy Management - Server”的设置。有关详细信息，请参阅修改 AGPM 服务。

组策略软件安装无法安装软件

- **原因**：AGPM 保留了组策略安装软件包的完整性。尽管对 GPO 进行了脱机编辑，但除缓存的客户端信息外的数据包之间的链接将保留。这是由设计原因引起的。
- **解决方案**：使用 AGPM 脱机编辑 GPO 时，配置其他 GPO 中数据包的任何组策略软件安装升级以引用已部署 GPO 而不是签出的副本。编辑必须对已部署 GPO 拥有**“读取”**权限。

将存档还原到新 AGPM 服务器时发生错误

- **原因**：由于安全原因，如果存档已移到另一台计算机，则为保护在**“域委托”**选项卡上输入的密码而进行的加密会导致密码失败。
- **解决方案**：在**“域委托”**选项卡上重新输入密码并确认。有关详细信息，请参阅配置电子邮件通知。

用户界面：Advanced Group Policy Management

使用 高级组策略管理 (AGPM) 可以将**“更改控制”**文件夹添加到在**“组策略管理控制台”**(GPMC) 显示的每个域中。在使用 GPMC 管理多个域的环境中，每个域都在控制台树的**“域”**文件夹下列出。每个域下都有一个**“更改控制”**文件夹，每个域还有 组策略对象 (GPO) 的一个存档。

在详细信息窗格中，有四个主要选项卡，提供对 AGPM 的 GPO 级别设置和域级别设置及命令的访问权限。此外，还有特定于 AGPM 的管理模板设置。

- 内容选项卡：GPO 设置和命令及 GPO 级别委派
- 域委托选项卡：AGPM 电子邮件通知设置和域级别委派
- AGPM 服务器选项卡：域级别存档连接设置
- “生产委托”选项卡：生产环境委派
- 管理模板文件夹：日志记录和跟踪的中央配置、存档位置和功能可见性

内容选项卡

“更改控制”窗格上的**“内容”**选项卡提供对 组策略对象 (GPO) 的访问和用于管理 GPO 的快捷菜单。右键单击项目时所显示的选项取决于您在被管理的 GPO 中的角色、权限和所有权。此外，这些快捷菜单因被管理的 GPO 的状态而异。

下列次级选项卡会筛选显示的 GPO 列表：

- **受控**：受 高级组策略管理 (AGPM) 管理的 GPO
- **非受控**：不受 AGPM 管理的 GPO
- **挂起**：等待审批者批准的 GPO 更改
- **模板**：用于创建新 GPO 和与现有 GPO 比较的 GPO 模板
- **回收站**：已删除的 GPO

“内容”选项卡及其次级选项卡提供有关每个 GPO 的详细信息以及对每个 GPO 历史记录的访问：

- 内容选项卡功能
- 历史记录窗口

右键单击任何次级选项卡上的 GPO，会显示该选项卡特有的快捷菜单，其中含有用于管理 GPO 的命令：

- 受控 GPO 命令
- 非受控 GPO 命令
- 挂起 GPO 命令
- 模板命令
- 回收站命令

其他参考

- 用户界面：Advanced Group Policy Management

内容选项卡功能

“内容”选项卡中的每个次级选项卡都包含两部分 -**“组策略对象”**和**“组和用户”**。

组策略对象部分

“组策略对象”部分显示 组策略对象 (GPO) 的筛选列表，还标识各个 GPO 的下列属性。可以使用**“搜索”**框搜索具有特定属性的 GPO。有关详细信息，请参阅搜索和筛选 GPO 列表。

GPO 属性	描述
名称	GPO 的名称。
状态	所选 GPO 的状态
更改者	签入所选 GPO 的编辑或部署所选 GPO 的审批者。
更改日期	对于受控 GPO，更改日期是进行修改后签入或签出后进行修改的最新日期。对于非受控 GPO，更改日期是上次进行修改的日期。
注释	由签入或部署 GPO 的人员在进行修改时输入的注释。当需要回滚到早期版本时，注释可用于识别特定版本。
计算机版本	自动生成的 GPO 计算机配置部分的版本。
用户版本	自动生成的 GPO 用户配置部分的版本。
GPO 状态	可以分别管理计算机配置和用户配置。GPO 状态可指示 GPO 的哪些部分已启用。
WMI 筛选器	显示应用于此 GPO 的所有 WMI 筛选器。可以在 GPMC 控制台树中域的**“WMI 筛选器”**文件夹下管理 WMI 筛选器。

组和用户部分

选择一个 GPO 后，在**“组和用户”**部分中会显示拥有该 GPO 访问权限的组和用户的列表。显示每个组或用户的允许权限和继承。AGPM 管理员 可以使用标准 AGPM 角色（编辑、审批者、审阅者和 AGPM 管理员）来配置权限或自定义组合的权限。

按钮	效果
添加	添加安全性描述符的新条目。可以添加 Active Directory 中的任何用户或组。
删除	从“访问控制列表”中删除所选条目。

按钮	效果
属性	显示所选对象的属性。该属性页与**“Active Directory 用户和计算机”**中对象的属性页相同。
高级	打开**“访问控制列表编辑器”**。

其他注意事项

- 有关与特定任务相关的角色和权限的信息，请参阅执行 AGPM 管理员任务、执行编辑任务、执行审批者任务和执行审阅者任务下的任务。

其他参考

- 内容选项卡

历史记录窗口

通过双击 GPO 或右键单击 GPO 后单击**“历史记录”**，可以显示 组策略对象 (GPO) 的历史记录。它还作为每个 GPO 的一个选项卡显示在 组策略管理控制台 (GPMC) 中。

历史记录提供了所选 GPO 生存期中的事件记录。从**“历史记录”**窗口中，您可以获取某个 GPO 版本中的设置报告，对多个版本的 GPO 进行比较，或者可以回滚到早期版本的 GPO。

在历史记录窗口中筛选事件

使用**“历史记录”**窗口中的选项卡，可以筛选 GPO 历史记录中的状态。

选项卡	筛选
所有状态	显示 GPO 历史记录中的所有状态。
特有版本	只显示 GPO 已签入存档的特有版本。此列表中省略了生产环境中部署的版本、到特有版本的快捷方式及信息状态。

事件信息

提供 GPO 历史记录中每种状态的信息。

GPO 属性	描述
更改日期	执行**“状态”**列中的操作时的时间标记。
状态	GPO 历史记录中的状态。
更改者	签入或部署 GPO 的人员。
注释	签入或部署 GPO 的人员在更改此版本时输入的注释，当需要回滚到早期版本时，注释可用于识

GPO 属性	描述
	别特定版本。
可删除	如果在存档中保留的每个 GPO 特有版本的数目是有限的，此版本的 GPO 是否可删除。 **备注** 通过右键单击 GPO，然后单击**“不允许删除”**或**“允许删除”**，可以更改是否可删除某个版本的 GPO。
计算机版本	自动生成的 GPO 计算机配置部分的版本。
用户版本	自动生成的 GPO 用户配置部分的版本。
GPO 状态	可以单独管理计算机的配置和用户配置。此状态显示已启用的 GPO 部分。
源 GPO 信息	对于已从其他林中导入的 GPO，原始 GPO 名称、域、用户和日期与上次更改相关。

报告

“设置”和**“差异”**按钮显示关于所选 GPO 版本 GPO 设置的报告。此外，右键单击 GPO 版本还会提供用于显示基于 XML 报告的选项。

按钮	效果
设置	生成基于 HTML 的报告，显示所选 GPO 版本中的设置。
差异	生成基于 HTML 的报告，对多个所选 GPO 版本中的设置进行比较。

差异报告中的关键字

符号	意义	颜色
无	同时存在于两个 GPO 中，具有相同设置的项目	随级别变化
[#]	同时存在于两个 GPO 中，但具有不同的设置的项目	蓝色
[-]	仅存在于第一个 GPO 中的项目	红色
[+]	仅存在于第二个 GPO 中的项目	绿色

- 对于具有不同设置的项目来说，当展开项目时会标识出不同设置。在每个 GPO 中显示属性值的顺序与在报告中显示 GPO 的顺序相同。
- 对设置进行某些更改后，可能导致将一个项目报告为两个项目（一个仅存在于第一个 GPO 中，另一个仅存在于第二个 GPO 中），而不是报告为一个已更改的项目。

其他参考

- 内容选项卡

受控 GPO 命令

“受控”选项卡：

- 显示受 高级组策略管理 (AGPM) 管理的 组策略对象 (GPO) 的列表。
- 提供包含管理 GPO 和显示 GPO 历史记录与报告的命令的快捷方式菜单。
- 显示有权访问选定 GPO 的组和用户的列表。

右键单击此选项卡上的**“组策略对象”**列表会显示一个快捷菜单。该菜单中包含下列适用的选项。

控制和历史记录

命令	效果
新建受控 GPO	使用通过 AGPM 管理的更改控制创建新 GPO，并将该 GPO 部署到域的生产环境。如果您没有创建 GPO 的权限，系统会提示您提交请求。（如果右键单击**“组策略对象”**列表时没有选择 GPO，则会显示此选项。）
历史记录	打开列出存档中保存的所选 GPO 的所有版本的窗口。从历史记录中，您可以获取某个 GPO 中的设置报告，比较两个版本的 GPO，将 GPO 与模板进行比较，或者可以回滚到早期版本的 GPO。

报告

命令	效果
设置	生成显示所选 GPO 中的设置的基于 HTML 或基于 XML 的报告，或者显示自最近控制、导入或签入 GPO 起从组织单位到所选 GPO 的链接。
差异	生成基于 HTML 或基于 XML 的报告，该报告比较两个选定的 GPO 内或选定的 GPO 和模板内的设置。

编辑

命令	效果
编辑	打开**“组策略管理编辑器”**窗口，更改所选 GPO。
签出	从存档中获取所选 GPO 的副本以进行脱机编辑，并在将该副本签入回存档之前，阻止其他任何人编辑该 GPO。签出可以由 AGPM 管理员（完全控制） 覆盖。
签入	将所选 GPO 的已编辑版本签入存档，以便其他授权编辑可以进行更改，或者审批者可以将该 GPO 部署到域的生产环境。
撤消签出	在未进行任何更改情况下将签出的 GPO 返回存档。

版本管理

命令	效果
从生产导入	对于所选 GPO，将域的生产环境中的版本复制到存档。
从文件导入	使用 GPO 备份文件的策略设置替换所选的已签出 GPO 的策略设置。
删除	将所选 GPO 移动到“回收站”，并指示是在生产中保留已部署版本（如果存在），还是删除存档中的版本以外的已部署版本。如果您没有删除 GPO 的权限，系统会提示您提交一个请求。
部署	将所选的已签入到存档的 GPO 移动到域的生产环境。此操作会在网络上激活它，还会覆盖 GPO 的先前激活版本（如果存在）。如果您没有部署 GPO 的权限，系统会提示您提交一个请求。
导出到	将所选 GPO 保存到备份文件，以便您可以将其复制到其他域。
标签	用说明性标签（如“已知正确”）和记录保存注释为所选 GPO 做标记。标签显示在**“状态”**列中，注释显示在**“历史记录”**窗口的**“注释”**列中。标签和注释可帮助您识别早期版本的 GPO，以便您可以在出现问题时进行回滚。

命令	效果
重命名	更改所选 GPO 的名称。如果已部署 GPO，则重新部署该 GPO 时，将在域的生产环境中更新其名称。
另存为模板	根据所选 GPO 的设置创建新模板。

杂项

命令	效果
刷新	更新组策略管理控制台 (GPMC) 的显示内容以包含所有更改。某些更改只有在刷新显示内容后才可见。
帮助	显示 AGPM 帮助。

其他参考

- 内容选项卡
- 执行编辑任务
- 执行审批者任务
- 执行审阅者任务

非受控 GPO 命令

“非受控”选项卡：

- 显示未受 高级组策略管理 (AGPM) 管理的 组策略对象 (GPO) 的列表。
- 提供包含将非受控 GPO 引入 AGPM 的管理之下和显示 GPO 历史记录与报告的命令的快捷方式菜单。
- 显示有权访问选定 GPO 的组和用户的列表。

右键单击此选项卡上的**“组策略对象”**列表会显示一个快捷菜单，其中包括下列适用的选项。

控制和历史记录

命令	效果
历史记录	打开列出存档中保存的所选 GPO 的所有版本的窗口。从历史记录中，您可以获取某个 GPO 中的设置报告，比较两个版本的 GPO，将 GPO 与模板进行比较，或者可以回滚到早期版本的 GPO。

命令	效果
控制	将所选非受控 GPO 引入 AGPM 的更改控制管理之下。如果您没有控制 GPO 的权限，系统会提示您提交一个请求。
另存为模板	根据所选 GPO 的设置创建新模板。

报告

命令	效果
设置	生成显示选定 GPO 内设置的基于 HTML 或基于 XML 的报告。
差异	生成基于 HTML 或基于 XML 的报告，该报告比较两个选定的 GPO 内或选定的 GPO 和模板内的设置。

杂项

命令	效果
刷新	更新组策略管理控制台 (GPMC) 的显示内容以包含所有更改。某些更改只有在刷新显示内容后才可见。
帮助	显示 AGPM 帮助。

其他参考

- 内容选项卡
- 执行编辑任务
- 执行审批者任务
- 执行审阅者任务

挂起 GPO 命令

“挂起”选项卡：

- 显示具有挂起 GPO 管理操作（如创建、控制、部署或删除）请求的 组策略对象 (GPO) 列表 。
- 提供具有响应挂起请求和显示 GPO 历史记录和报告的命令快捷方式菜单。
- 显示有权访问选定 GPO 的组和用户的列表。

右键单击此选项卡上的**“组策略对象”**列表会显示一个快捷菜单，其中包括下列适用的选项。

控制和历史记录

命令	**效果**
历史记录	打开列出存档中保存的所选 GPO 的所有版本的窗口。从历史记录中，您可以获取某个 GPO 中的设置报告，比较两个版本的 GPO，将 GPO 与模板进行比较，或者可以回滚到早期版本的 GPO 。
撤消	在批准请求之前，撤消挂起的创建、控制或删除所选 GPO 的请求。
批准	完成编辑创建、控制或删除所选 GPO 的挂起请求。
拒绝	拒绝编辑创建、控制或删除所选 GPO 的挂起请求。

报告

命令	**效果**
设置	生成显示所选 GPO 中设置的基于 HTML 或基于 XML 的报告，或者显示指向选定的最近控制、导入或签入 GPO 时组织单位的 GPO 链接。
差异	生成基于 HTML 或基于 XML 的报告，该报告比较两个选定的 GPO 内或选定的 GPO 和模板内的设置。

杂项

命令	**效果**
刷新	更新组策略管理控制台 (GPMC) 的显示内容以包含所有更改。某些更改只有在刷新显示内容后才可见。
帮助	显示 AGPM 帮助。

其他参考

- 内容选项卡

- [执行审批者任务]
- [执行审阅者任务]

模板命令

“模板”选项卡：

- 显示可用于创建新 组策略对象 (GPO) 的可用模板的列表。
- 提供其中包含命令的快捷菜单，这些命令用于基于选定模板创建 GPO、管理模板并显示模板的报告。
- 显示有权访问选定模板的组和用户的列表。

因为模板不能改变，所以模板没有历史记录。但是，像任何 GPO 版本一样，模板的设置可以使用设置报告加以显示，或使用差异报告与另一个 GPO 进行比较。

备注

模板是 GPO 的静态、不可编辑版本，可用作创建新的可编辑 GPO 的起始点。

右键单击此选项卡上的**“组策略对象”**列表会显示一个快捷菜单，其中包括下列适用的选项。

控制

命令	效果
新建受控 GPO	基于选定的模板创建新 GPO。提供有将新 GPO 部署到域的生产环境的选项。如果您没有创建 GPO 的权限，则系统会提示您提交请求。（如果右键单击**“组策略对象”**列表时没有选择 GPO，则会显示此选项。）

报告

命令	效果
设置	生成显示选定 GPO 内设置的基于 HTML 或基于 XML 的报告。
差异	生成一个比较两个选定 GPO 模板内设置的基于 HTML 或基于 XML 的报告。

模板管理

命令	效果
设为默认值	将选定的模板设置为在创建新 GPO 时自动使用

命令	效果
	的默认模板。
删除	将选定的模板移到**“回收站”**。如果您没有删除 GPO 的权限，则系统会提示您提交请求。
重命名	更改选定模板的名称。

杂项

命令	效果
刷新	更新组策略管理控制台的显示内容以包含所有更改。某些更改只有在刷新显示内容后才可见。
帮助	显示 高级组策略管理 (AGPM) 帮助。

其他参考

- 内容选项卡
- 执行编辑任务
- 执行审阅者任务

回收站命令

“回收站”选项卡：

- 显示已从存档中删除的 组策略对象 (GPO) 的列表。
- 提供一个快捷菜单，其中包含的命令可用于管理 GPO 和显示 GPO 的报告。
- 显示有权访问选定 GPO 的组和用户的列表。

右键单击此选项卡上的**“组策略对象”**列表会显示一个快捷菜单，其中包含下列适用的选项：

报告

命令	效果
设置	生成显示选定 GPO 内设置的基于 HTML 或基于 XML 的报告，或者显示自最近控制、导入或签入 GPO 后，指向组织单位中选定 GPO 的链接。
差异	生成基于 HTML 或基于 XML 的报告，该报告比较两个选定的 GPO 内或选定的 GPO 和模板内的设置。

版本管理

命令	效果
破坏	从**“回收站”**删除选定的 GPO，则该 GPO 将无法再还原。
还原	将选定的 GPO 从**“回收站”**移到**“受控”**选项卡。此操作不会将 GPO 还原到生产环境。

杂项

命令	效果
刷新	更新组策略管理控制台 (GPMC) 的显示内容以包含所有更改。某些更改只有在刷新显示内容后才可见。
帮助	显示 高级组策略管理 (AGPM) 帮助。

其他参考

- 内容选项卡
- 执行审批者任务
- 执行审阅者任务

域委托选项卡

在**“更改控制”**窗格中的**“域委托”**选项卡上，提供了对存档拥有域级别访问权的组策略管理员列表，并指出了每个组策略管理员的角色。此外，此选项卡使 AGPM 管理员（完全控制） 能够配置编辑、审批者、审阅者和其他 AGPM 管理员 的域级别权限。**“域委托”**选项卡上有两个部分，用于在域级别配置电子邮件通知，以及基于角色进行 高级组策略管理 (AGPM) 委派。

配置电子邮件通知

此选项卡上的电子邮件通知部分确定当 AGPM 中的操作挂起时将收到通知的审批者。

设置	描述
发件人电子邮件地址	将通知发送到审批者的 AGPM 别名。在多域环境中，整个环境中的别名可以相同，也可以在每个域使用不同的别名。
收件人电子邮件地址	将通知发送到的以逗号分隔的审批者电子邮件地址列表

设置	描述
SMTP 服务器	电子邮件服务器的名称，如 mail.contoso.com
用户名	对 SMTP 服务器具有访问权限的用户
密码	SMTP 服务器进行身份验证的用户密码
确认密码	确认用户密码

域级别基于角色的委派

此选项卡上基于角色的委派部分显示并启用 AGPM 管理员，以便为该域中拥有存档访问权限的每个组和用户委派允许、拒绝和继承的权限。AGPM 管理员 可以使用标准 AGPM 角色（编辑、审批者、审阅者和 AGPM 管理员）或每个组策略管理员的定制组合权限配置全域性权限。

按钮	效果
添加	添加安全性描述符的新条目。可以将 Active Directory 中的任何用户或组作为组策略管理员添加。
删除	从访问控制列表中删除所选组策略管理员。
属性	显示所选组策略管理员的属性。
高级	打开**“访问控制列表编辑器”**。

其他注意事项

- 有关与特定任务相关的角色和权限的信息，请参阅执行 AGPM 管理员任务、执行编辑任务、执行审批者任务和执行审阅者任务下的任务。

其他参考

- 用户界面：Advanced Group Policy Management
- 执行 AGPM 管理员任务

AGPM 服务器选项卡

使用**“更改控制”**窗格上的**“AGPM 服务器”**选项卡可以通过输入完全限定的计算机名称和端口来选择 AGPM 服务器，以及从存档中删除旧版 组策略对象 (GPO) 以节省 AGPM 服务器上的磁盘空间。

指定 AGPM 服务器

选定的 AGPM 服务器确定在**“内容”**选项卡上所显示的存档，以及确定将**“域委托”**设置应用到的位置。高级组策略管理 (AGPM) 的默认端口是端口 4600。

如果 AGPM 服务器连接是使用管理模板设置集中配置的，则此选项卡上用于配置连接的选项不可用。有关详细信息，请参阅配置 AGPM 服务器连接。

删除旧 GPO 版本

默认情况下，每个受控 GPO 的所有版本都会保留在存档中。但是，您可以配置 AGPM 服务以限制为每个 GPO 保留的版本数量，并在超出该限制时自动删除最旧的版本。此限制仅计算**“历史记录”**窗口的**“唯一版本”**选项卡上显示的 GPO 版本。

注意

为每个 GPO 存储的唯一版本的最大数量不包括当前版本，因此，输入 0 将仅保留当前版本。该限制不能大于 999 个版本。

当删除某个 GPO 版本后，该版本的记录会保留在 GPO 的历史记录中，但 GPO 版本本身会从存档中删除。您可以在历史记录中将某个 GPO 版本标记为不可删除来防止该 GPO 版本被删除。

其他参考

- 用户界面：Advanced Group Policy Management
- 执行 AGPM 管理员任务
- 执行审阅者任务

“生产委托”选项卡

在**“更改控制”**窗格中的**“生产委托”**选项卡上，提供了对生产环境中的受控 组策略对象 (GPO) 具有域级别访问权限的用户和组的列表，还指出了每个用户或组的允许权限。

此选项卡允许 AGPM 管理员（完全控制） 修改域的生产环境中 GPO 的默认委派访问权限，从而可以添加或删除用户和组，可以修改每个用户和组的允许权限。

按钮	效果
添加	添加安全性描述符的新条目。
删除	从“访问控制列表”中删除所选用户或组。
属性	显示所选用户或组的属性。该属性页与**“Active Directory 用户和计算机”**中对象的属性页相同。

其他参考

- 用户界面：Advanced Group Policy Management
- 执行 AGPM 管理员任务

管理模板文件夹

使用 高级组策略管理 (AGPM) 的管理模板设置，可以为要应用带这些设置的 组策略对象 (GPO) 的 AGPM 客户端和 AGPM 服务器集中配置日志记录和跟踪选项。同样，使用这些设置可以为要应用带这些设置的 GPO 的组策略管理员集中配置存档位置和**“更改控制”**文件与**“历史记录”**选项卡的可见性。

- 日志记录和跟踪的设置
- AGPM 服务器连接设置
- 功能可见性设置

其他参考

- 用户界面：Advanced Group Policy Management
- 执行 AGPM 管理员任务

日志记录和跟踪的设置

对于将管理模板设置应用于 组策略对象 (GPO) 的 AGPM 服务器和客户端，可以通过 高级组策略管理 (AGPM) 的这些设置集中配置日志记录和跟踪的选项。

当编辑 GPO 时，Computer Configuration\Policies\Administrative Templates\Windows Components\AGPM 下的以下设置可用。

跟踪文件位置：

- 客户端：%LocalAppData%\Microsoft\AGPM\agpm.log
- 服务器：%ProgramData%\Microsoft\AGPM\agpmserv.log

设置	效果
AGPM:配置日志记录	此策略设置允许打开和配置 AGPM 的日志记录。此设置影响 AGPM 的客户端和服务器组件。

其他参考

- 管理模板文件夹

AGPM 服务器连接设置

您可以使用 高级组策略管理 (AGPM) 的管理模板设置，为应用带有这些设置的 组策略对象 (GPO) 的组策略管理员集中配置 AGPM 服务器连接。

编辑 GPO 时，可以使用 User Configuration\Policies\Administrative Templates\Windows Components\AGPM 下的以下设置。

设置	效果
AGPM:指定默认 AGPM 服务器(所有域)	使用此策略设置可以指定所有域的默认 AGPM 服务器。这个设置仅由 AGPM 客户端使用，而且会

设置	效果
	限制组策略管理员连接到另一个存档。可以使用**“AGPM:指定 AGPM 服务器”**设置覆盖单个域的这一默认设置。
AGPM:指定 AGPM 服务器	使用此策略设置可以指定单个域的 AGPM 服务器。这个设置仅由 AGPM 客户端使用，而且会限制组策略管理员连接到指定域的其他存档。要指定默认 AGPM 服务器，请使用**“AGPM:指定默认 AGPM 服务器(所有域)”**设置，然后使用此策略设置覆盖每个域的默认设置。

其他参考

- 管理模板文件夹
- 执行 AGPM 管理员任务

功能可见性设置

对于将管理模板设置应用于 组策略对象 (GPO) 的组策略管理员，他们可以通过 高级组策略管理 (AGPM) 的这些设置集中配置**“更改控制”**文件夹和**“历史记录”**选项卡的可见性。

当编辑 GPO 时，User Configuration\Policies\Administrative Templates\Windows Components\Microsoft Management Console\Restricted/Permitted Snap-ins\Extension Snap-ins 下的以下设置可用。

设置	效果
AGPM:显示“更改控制”选项卡	此策略设置允许您控制组策略管理控制台 (GPMC) 中**“更改控制”**文件夹的可见性。
AGPM:显示所链接 GPO 的“历史记录”选项卡	此策略设置允许您在查看 GPMC 中链接的 GPO 时，控制由 AGPM 提供的**“历史记录”**选项卡的可见性。
AGPM:显示 GPO 的“历史记录”选项卡	此策略设置允许您在查看 GPMC 中 GPO 时，控制由 AGPM 提供的**“历史记录”**选项卡的可见性。

其他参考

- 管理模板文件夹